Master Thesis
Computer Science
Thesis no: MCS-2011-03
January 2011

Enhancing Information Security in Cloud Computing Services using SLA Based Metrics

Nia Ramadianti Putri
Medard Charles Mganga

School of Computing
Blekinge Institute of Technology
SE – 371 79 Karlskrona
Sweden

This thesis is submitted to the School of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Author(s):
Nia, (Ramadianti), Putri
E-mail: niaramadianti@gmail.com

Medard, (Charles), Mganga
E-mail: mgangacm@gmail.com

University advisor(s):
Prof. Rune Gustavsson
School of Computing

School of Computing
Blekinge Institute of Technology
SE – 371 79 Karlskrona
Sweden

Internet : www.bth.se/com
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

ABSTRACT

Context: Cloud computing is a prospering technology that most organizations are considering for adoption as a cost effective strategy for managing IT. However, organizations also still consider the technology to be associated with many business risks that are not yet resolved. Such issues include security, privacy as well as legal and regulatory risks. As an initiative to address such risks, organizations can develop and implement SLA to establish common expectations and goals between the cloud provider and customer. Organizations can base on the SLA to measure the achievement of the outsourced service. However, many SLAs tend to focus on cloud computing performance whilst neglecting information security issues.

Objective: We identify threats and security attributes applicable in cloud computing. We also select a framework suitable for identifying information security metrics. Moreover, we identify SLA based information security metrics in the cloud in line with the COBIT framework.

Methods: We conducted a systematic literature review (SLR) to identify studies focusing on information security threats in the cloud computing. We also used SLR to select frameworks available for identification of security metrics. We used Engineering Village and Scopus online citation databases as primary sources of data for SLR. Studies were selected based on the inclusion/exclusion criteria we defined. A suitable framework was selected based on defined framework selection criteria. Based on the selected framework and conceptual review of the COBIT framework we identified SLA based information security metrics in the cloud.

Results: Based on the SLR we identified security threats and attributes in the cloud. The Goal Question Metric (GQM) framework was selected as a framework suitable for identification of security metrics. Following the GQM approach and the COBIT framework we identified ten areas that are essential and related with information security in the cloud computing. In addition, covering the ten essential areas we identified 41 SLA based information security metrics that are relevant for measuring and monitoring security performance of cloud computing services.

Conclusions: Cloud computing faces similar threats as traditional computing. Depending on the service and deployment model adopted, addressing security risks in the cloud may become a more challenging and complex undertaking. This situation therefore appeals to the cloud providers the need to execute their key responsibilities of creating not only a cost effective but also a secure cloud computing service. In this study, we assist both cloud provider and customers on the security issues that are to be considered for inclusion in their SLA. We have identified 41 SLA based information security metrics to aid both cloud providers and customers obtain common security performance expectations and goals. We anticipate that adoption of these metrics can help cloud providers in enhancing security in the cloud environment. The metrics will also assist cloud customers in evaluating security performance of the cloud for improvements.

Keywords: cloud computing, security metrics, security threats, security measurement frameworks

ACKNOWLEDGEMENTS

We would like to express our gratitude to our thesis supervisor, Prof. Rune Gustavsson, whose expertise, guidance and support enabled us to develop understanding of the study. We would like to thank our families and friends who provided us with support and encouragement throughout this study. Without them we would not have been able to complete this thesis.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

As more and more demands for Information Technology (IT) services rise, there are also increasing needs to expand IT architecture and infrastructures to provide more services. As a consequence, IT service providers are faced with challenges of expanding the structures and infrastructures with small expenditure and minimum time in order to provide rising demands from their customers. To address these business challenges and commercial interests, cloud computing architecture was developed. Cloud computing architecture is an environment of IT resources for particular services which is outsourced to customers [1]. In the context of cloud computing, the cloud service provider is known as cloud provider which is an organization that provides cloud computing service. On the other hand the organization that receives the cloud computing service is known as the cloud customer. Cloud computing is not a novel concept, however it is rising now and it will have major role in the next 10 years or more [1]. It is an increasing concept because of several reasons including reduction in cost and energy consumption of the shared computing resources (servers, software, storage, and networking)[2]. It also enables effective IT resources usage and increases flexibility for expanding new infrastructures in instant time [2].

Like traditional computing environments, cloud computing brings risks and security concerns to the business that need to be considered appropriately. Such risks and security concerns include challenges in handling privileged user access, ensuring legal and regulatory compliance, ensuring data segregation, maintaining data recovery, difficulty in investigating illegal activities, and lack of assurance of long-term viability of the cloud provider [3] . Due to these challenges cloud customers therefore need to institute mechanisms to measure and improve security of their information assets operating in the cloud. Among the alternatives available to the cloud customer for monitoring, measuring and hence improving information security of the assets managed in the cloud is to develop information security metrics.

Since cloud computing resources are delivered as a service, cloud customer therefore can implement the information security metrics through a Service Level Agreement (SLA). SLA is a legal agreement between a service provider and the customer [4] and is the main basis for managing and controlling the rendered services. SLA metrics are therefore used to assess service level between cloud provider and its customers and serve as basis for service improvement [4]. However, the trend among existing cloud SLAs focuses more on performance measurement than on security measurement. Example of these SLA include a the GoGrid SLA [5]. Among the issues that hinder the organization from adopting the cloud computing is information security risks [6] [7]. However, we still experience cloud providers not addressing it [6] [7].

We recognize that several studies have been conducted on security metrics, cloud computing as well as SLA. However, none of these studies focused on SLA based information security metrics particularly for cloud computing.

In this study, we therefore select a framework that is suitable to identify information security metrics. We then review the COBIT document and follow the selected framework to identify SLA based information security metrics in cloud computing.

1.1 Aims

The overall aim of this study is to identify SLA based information security metrics in cloud computing using the COBIT framework.

1.2 Objectives

The set objectives of the study which will direct towards achieving our aim are to:

i) Identify relevant information security attributes for cloud computing

ii) Identify information security threats for cloud computing

iii) Select a framework suitable for developing security metrics

iv) Identify SLA based information security metrics in cloud computing aligned with the COBIT framework

1.3 Terminologies

This subsection provides a better understanding of terminologies used in the study as presented in table 1.

Table 1: Terms and definitions used in the study

Terms	Definitions
Cloud computing	Cloud computing refers to a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction) [8].
Cloud provider	Often also called Cloud Service Provider (CSP) [9], it is an external enterprise or organization that offers cloud services to its customers [1]. Cloud provider is paid by its costumers based on cloud service usage with pay-per-use scheme [1].
Cloud customer	Customers who make direct use of cloud services [1]. In this study the customers are organizations rather than personals.
IT asset	Refers to information, technology and people owned by an organization [10].
Change request	Refers to the duration taken for the configuration changes to take effect in the cloud system [11].
Computer Security Incident	A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices [12].
IT non-compliance	Breaches of any legal (law, regulatory or contractual) business obligations and/ or IT policies and standards [10] [9].
Security vulnerabilities	Flaws in the process of design and implementation for software, hardware, and protocol for the computer system or on the system security policy [13].
Security patches and fixes	Security preventative and corrective measures respectively integrated over the leased cloud system to defend information systems and its technologies from the attack of malicious software (spyware, virus, etc) [10].
Problems	Problem in IT environment means an unknown underlying cause of one or multiple incidents [10] [14].
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring [12].
Information Security attributes	information security components or qualities that satisfy the business objectives [10]. Information security attributes may include confidentiality, integrity, availability, accountability, non-repudiation, authenticity, privacy, etc. However the attributes relate to this study are confidentiality, integrity, availability and accountability.
Senior manager	A person holding a top management position in an organization who is responsible for making strategic decisions for achieving intended organization's business objectives.

2 BACKGROUND

This section is dedicated to provide an overview concerning concepts used in this study. Section 2.1 discusses about cloud computing and 2.2 presents information about Service Level Agreement (SLA). Section 2.3 discusses about Control Objectives for Information and related Technology (COBIT). Goal Question Metric (QGM) framework is presented in section 2.4 followed by information security in section 2.5. Lastly, brief information about security metrics is presented in section 2.6.

2.1 Cloud computing

Cloud computing is considered a new method of distributing computer resources [15].These resources are usually distributed as services [16]. The cloud computing service architecture falls under three categories of services and there exist four deployment models [8]. The services posses own unique fundamental characteristics that distinguish them from the traditional computing environment. Therefore, in this section we present cloud computing characteristics, services and deployment models.

2.1.1 Cloud computing characteristics

Cloud computing has five fundamental characteristics as follows [8]:

i. On-demand self-service.

Cloud customers can demand computing capabilities such as network storage [8].

ii. Broad network access.

The cloud capabilities are available over the network and are accessed by customers using platforms (e.g.: laptop, PDA) [8].

iii. Resource pooling.

Cloud provider's computing resources are pooled to support multiple users or multi-tenancy model [8].

iv. Rapid elasticity.

The capabilities can be rapidly and elastically demanded [8]. The capabilities are appeared to be infinitely available to the customers and can be purchased at any time [8].

v. Measured service.

Cloud system automatically controls and optimizes the resources usage by leveraging metering capability to the specific type of service. (e.g. Bandwidth, storage) [8]. Resource usage is controlled, monitored and reported providing transparency for both cloud provider and customer [8].

2.1.2 Cloud computing services

Cloud computing services or cloud services are typically categorized into three types namely Software as a Service (SaaS), Platforms as a Service (PaaS) and Infrastructure as a Service (IaaS) [9]. These three categories offer different services to cloud customers. Usually, cloud customers can demand on the type of services they require [9] [17]. Brief description of the three services will be presented in the subsequent sections. An illustration of cloud services architecture is as presented in figure 1.

i. Software as a Service (SaaS).

In SaaS, customers are renting complete applications instead of purchasing and installing the applications or software on their computers [9] [17] [18]. SaaS

provider hosts the applications and makes the applications available over the network [17]. SaaS applications are multi-tenant applications which means that the applications are shared to multiple customers [9]. However the applications are logically unique for each customer [9].

It is the responsibilities of the provider to secure customers information in SaaS [9]. Several examples of SaaS applications are online word processing tools and web content delivery services [15]. Companies that offer SaaS services include Google and Salesforce.com

ii. Platforms as a Service (PaaS).

In PaaS service, cloud provider offers a platform for development environment to the customers to run their applications [9] [19]. The development platform is Application Programming Interface (API) and is configurable remotely [15]. The platform service includes configuration management, deployment platform and development tools [9] [15]. Therefore, customers can run their applications without having specialized administration skills [9]. Further, the customers can build and deploy their web applications without having to install any tools on their computers [9].

Similar to SaaS, PaaS provider is responsible for securing the leased services [9]. PaaS security spans between two software layers [9]:

- Security of PaaS platform itself. For instance: runtime engine that is integrated in PaaS service.
- Security of client applications which are running on PaaS platform.

Therefore, the PaaS provider is responsible for securing the platform and the customer's applications. Companies that offer PaaS service include Microsoft Azure and Google App Engine [9].

iii. Infrastructure as a Service (IaaS).

IaaS service offers virtual machines as well as other abstracted hardware and operating system over the network [1] [9] [15] [20]. By renting IaaS service, the customers can use the latest infrastructure technology and they do not have to concern with updating the technology [20]. Contrast to SaaS and PaaS, customers of IaaS are mainly responsible for securing the leased infrastructure [9]. Companies that offer this service include GoGrid, Flexiscale, and Amazon.

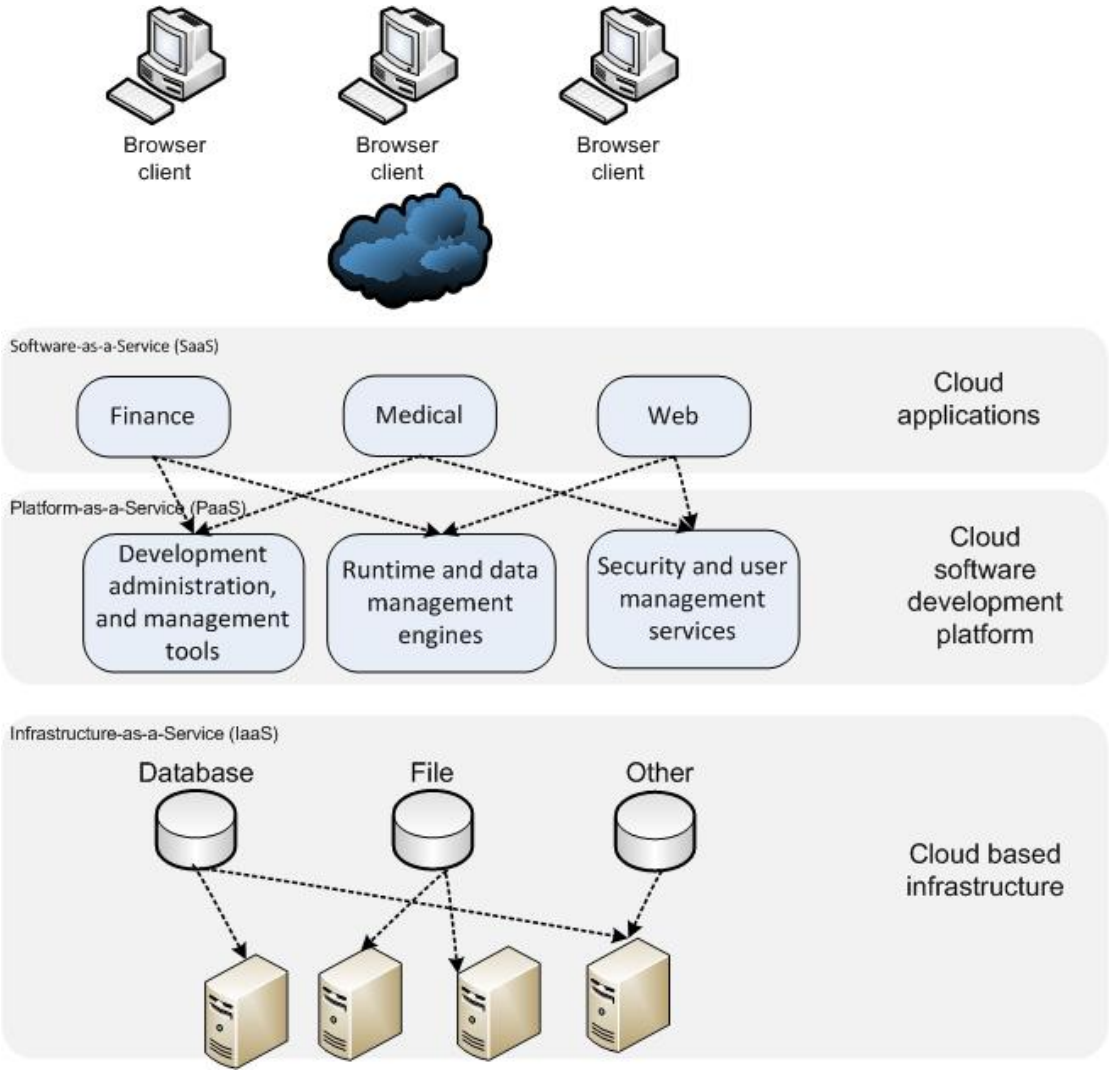

Figure 1: Cloud services architecture [9]

2.1.3 Cloud Deployment Model

Similar to type of service, cloud may be hosted and deployed in different fashions depending on the use case [1]. Cloud deployment models are as follows:

i. *Private cloud*

   In private cloud model, the cloud infrastructure is deployed merely for single organization [8].

ii. *Community cloud*

   In community cloud model, the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns [8].

iii. Public cloud

In public cloud model, the cloud infrastructure is made available to public or a large industry group [8]. The cloud is owned by an organization that sells service [8].

iv. Hybrid cloud

In hybrid model, the cloud infrastructure is a composition of two or more clouds (private, community, or public) [8].

2.2 Service Level Agreement (SLA)

SLA is a written agreement about service levels offered by providers to customers [19]. In the context of this study, SLA is an agreement between cloud providers and cloud customers. Main advantage of SLA is to gain common understanding of various issues including service levels and responsibilities of provider and customer [19]. The stated issues and service levels in SLA depend on negotiation between provider and customer.

According to Chaves et al. [19] SLA defines the "what" and not the "how". It means in regards to information security, SLA states what type of service levels customer should receive. However it does not state how the service levels are achieved [19]. SLA also provides information about responsibilities of both cloud provider and customer towards unexpected events that happen to the service [19].

In cloud computing, customers delegate their information to cloud provider and they are not aware of where their information are stored and processed [3]. Hence, cloud provider needs to use SLA to convince customers to use their services and to assure the security of their information. SLA for cloud computing should embrace wide range of issues starting from performance to security issues [3]. In this study the SLA considered is service levels related to information security in cloud computing environment.

2.3 Control Objectives for Information and related Technology (COBIT)

One framework that proposes SLA metrics is COBIT framework. COBIT [10] framework is a set of comprehensive open documents to assure sound IT governance in an organization [21]. COBIT covers complete governance, control and assurance over IT. It is a business-focused, process-oriented, controls-based and measurement-driven framework [10]. IT governance concerns with integration and incorporation of good practices to ensure that IT resources support the business objectives [10]. Effective IT governance ensures that IT functions can sustain business strategies and objectives of an organization and appropriately manages IT-related risks [10] [22]. Since IT governance is the responsibility of IT managerial level [10] therefore COBIT helps them in executing their duties of managing IT. It also aids IT professionals in auditing/assessing internal controls in an organization [23].

COBIT is developed within a basic principle that is intended to provide organizations with information required in achieving their business objectives while managing IT investment and resources [10]. This principle is as illustrated in figure 2. In general, an organization needs to control and manage its IT resources to achieve its objectives.

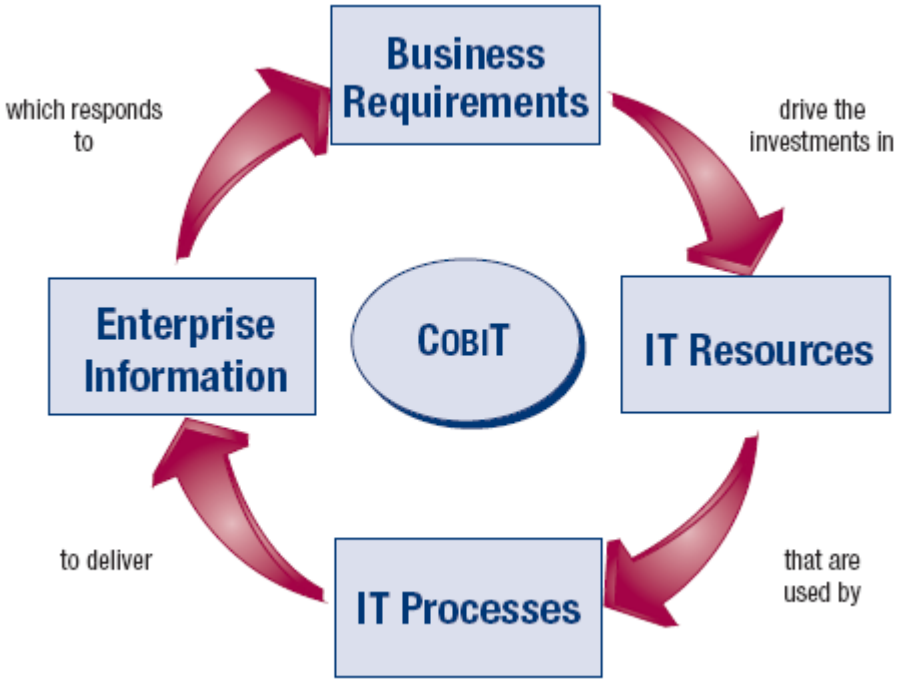

Figure 2: Basic Principle of COBIT [10].

COBIT framework is globally recognized mainly because it aligns IT functions with business goals of an organization [21]. COBIT is increasingly used to control and assure information system operations [23]. It is referred as one of the successful security management framework implemented in big enterprise [24]. In addition COBIT has long history of being used as an auditing reference by IT professionals [23] [25]. COBIT can be used by itself or in conjunction with other IT- related frameworks and standards [21] such as ISO/IEC 27001 (ISO 27001), IT Infrastructure Library (ITIL), and National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series.

COBIT framework presents guidelines to derive metrics for IT governance processes that align with business goals. In this study we follow COBIT framework to derive SLA based information security metrics in cloud computing.

2.4 Goal Question Metric (GQM) framework

To complete this study particularly phase 3 (developing security metrics from COBIT), GQM framework is followed to aid in identifying SLA based information security metrics. GQM framework is a structured and widely accepted method to answer questions of what to measure [26]. It is a goal-oriented measurement framework which means the measurement starts with goals [27]. To measure an object, organization needs to define the measurement goals which are based upon the organization goals [27]. Then each goal is refined into several questions which breaks down the issue found in the object into several components [27] [28]. These questions also characterize the way the measurement is performed [26] [28]. Thereafter, each question is refined into several metrics which provide information to answer each question [27]. The end result of conducting GQM is specification of measurement system targeting particular issues and rules for the interpretation of the measurement data [28]. The GQM framework consists of three main levels namely conceptual (goal), operational (question) and quantitative (metric) [28]:

2.4.1 Conceptual level (goal)

The goal needs to be specified for the targeted object [28]. Goal comprises purpose of measurement, object to be measured, issue to be measured and viewpoint of which the measurement is taken from [28]. The goal then is refined into several questions in operational level.

Object of measurement may be [28]:

- Products: Artifacts, deliverables and documents in which the outcomes of during the system life cycle. E.g.: designs, programs, specifications.
- Processes: Software activities which are typically associated with time. E.g.: Designing, interview, specifying.
- Resources: Items used by process to produce their outputs. E.g.: hardware, software, employee, office space.

2.4.2 Operational level (question)

This level comprises a set of questions used to characterize the way the measurement of a specific goal is taken [28]. These questions try to characterize the object of measurement (products/processes/resources) with the particular issue and viewpoint [28].

2.4.3 Quantitative level (metric)

The quantitative level involves refining the questions into a set of metrics/measurements [28]. A set of metrics intended to answer specific question in quantitative way [28]. The same metrics can be used to answer different questions under the same goal [28].

The metrics can be [28]:

- Objective: If the metrics base only on the object of measurement and not from viewpoint of measurement
- Subjective: If the metrics base on both object of measurement and the viewpoint of measurement.

The illustration of GQM framework is presented below in figure 3.

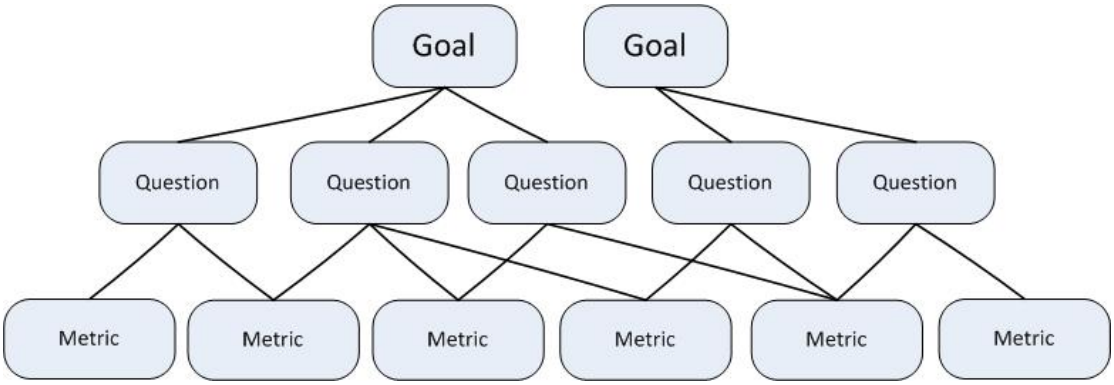

Figure 3: GQM framework [28]

2.5 Information security

SysAdmin, Audit, Network, Security (SANS) [29] defines information security as processes and methodologies which are intended to protect sensitive information or data from unauthorized access, disclosure, modification, or use. The form of the protected data or information can be electronic, printed, or other forms [29].

Information security encompasses three fundamental security attributes namely confidentiality, availability and integrity [30]. The presence of these attributes characterizes a secured information [30]. Besides these three fundamental attributes, non-repudiation and accountability complement the characteristic of secured information [30]. The five attributes of information security are shown in figure 4.

Figure 4: Security attributes (inspired by [30])

The five attributes described as follows:

i. Confidentiality.

This attribute concerns with protecting the sensitive information from the unauthorized disclosure [10].

ii. Integrity.

This attribute concerns with accuracy, completeness and validity of information in regards with business requirement and expectations [10].

iii. Availability.

This attribute concerns with information being operational and accessible whenever it is required by the business process now as well as in the future [10] [30]. Further, the information must be inaccessible to unauthorized users [30].

iv. Accountability.

This attribute concerns with keeping track of actions that are related to security actions and responsibilities [30].

v. Non-repudiation.

This attribute concerns with the ability to prevent users from denying the responsibility of the actions performed [30].

2.6 Security metrics

Security metrics are quantitative measurements to assess security operations in organization environment [31]. They aid the organization to make decisions about various aspects of security which include security architectures and controls to the effectiveness and efficiency of security operations [32]. Moreover, security metrics are valuable to IT managerial level and stakeholders who are questioning the security impacts towards business process and activities [33]. Further, security operations frequently demand high expenditures and with security metric it provides comprehensible reasons of the security high expenditures to the managerial level and stakeholders [33].

NIST [34] characterizes security metrics into three types as follows:

i. Implementation metrics.

These metrics are intended to demonstrate progress in implementing information security programs, security controls, and related policies and procedures [34].

ii. Effectiveness/efficiency metrics.

These metrics are intended to monitor if the program-level processes and system-level security controls are implemented correctly, operating as intended as well as meeting the desired outcomes [34].

iii. Impact metrics.

These metrics are intended to articulate the impact of information security on an organization's mission [34].

Security metrics may be divided also based on their uses. The uses of security metrics are categorized into strategic support, quality assurance and tactical oversight [32] [33]. In this study, we follow the three types of metrics defined by NIST [34].

3 RELATED WORK

Several studies have been conducted in the area of SLA metrics, security metrics and cloud computing. Several SLA metrics have been proposed. For instance, Skita et al. [35] propose SLA metric for real-time application on grid architecture. Jain et al. [36] propose SLA management system over IP networks.

In the area of cloud computing several researches have also been conducted. For example, Stantchev [37] proposes an approach of performance evaluation of cloud computing configurations. Rimal and Choi [20] surveyed on architectural approaches of cloud computing system and identified potential further research in cloud computing area.

Moreover, different approaches have been followed in developing security metrics. For instance, Tash and Ghernaouti [38] propose a framework that uses risk assessment to derive efficient metrics for measuring information security. Tanna et al. [39] propose a model for identifying metrics based on threat model. Another approach is the one described by SANS [40] which presents seven steps for generating security metrics.

In addition, different taxonomies for security metrics have been proposed. For instance, the well known NIST [34] presents three broader categories of security metrics namely implementation, effectiveness/efficiency and impact. A more comprehensive taxonomy of security metrics is presented by Savola [41] . Savola [41] performed a literature survey on existing security metrics taxonomy and proposes another taxonomy. Among the taxonomy presented by Savola [41] includes assurance metrics consisting of organization security metrics and metrics for Technical Target of Assessment.

Although there are several different approaches for developing security metrics not all approaches have been successful and accepted in the industry. This argument is supported by Tash and Ghernaouti [38] who argue that security practitioners often develop technical security metrics which cannot be used to measure organization security. The authors further suggest that security frameworks such as ISO 17799:2005, ISO 27001 and COBIT may be used to derive security measures for evaluation of overall organization security [38].

Despite existence of several researches on SLA metrics and cloud computing areas, to the best of our knowledge there is no research conducted to determine SLA based information security metrics in cloud computing which is our main contribution. Another contribution of the study is on the identification of a framework suitable for developing information security metrics.

4 METHODOLOGY

Research questions, research methodologies and research plan are presented in this section.

4.1 Research questions

To achieve aims and objectives stated in sections 1.1 and 1.2 respectively, these following research questions are addressed:

RQ1. What information security attributes are relevant in cloud computing?

This research question is formulated in order to identify information security attributes relevant in cloud computing. The answers to this question also assist us to identify information security metrics in cloud computing as required in RQ3. The RQ1 is indirectly answered through RQ 1.1.

RQ1.1 What information security threats are relevant in cloud computing?

The main objective of this research question is to understand information security threats relevant in cloud computing. In addition, the answers to this question will enable us to be focused on cloud computing issues when identifying information security metrics rather than the traditional computing environment.

RQ2. Which framework is suitable for developing security metrics?

This research question aims at selecting a framework that will be followed in identifying information security metrics. This is important because several frameworks might be found in literature some of which may not be effective in identifying security metrics. This is also important because in the absence of a suitable framework numerous information security metrics might be found in the study hence becoming unmanageable.

RQ3. What are SLA based information security metrics in cloud computing?

This research question is the main focus of the study. We use the framework selected in RQ2 together with the results from RQ1 to identify SLA based information security metrics in cloud computing. The identified metrics will be useful to those organizations operating in the cloud which intend to measure information security stand of their computing environments.

4.2 Research methods and rationale

We conduct two methods in this study, systematic literature review (SLR) and thorough analysis of COBIT framework. The rationales for conducting these methods are as follows:

4.2.1 Rationale for systematic literature review

According to Jeffery and B. Neidecker-Lutz [1] cloud computing is emerging in Europe at this moment. Hence there is less information to collect from industry practitioners. For this reason we only rely on information from literature to attain some of the objectives of this study. We therefore collect data required in this study through SLR. We adopt SLR as proposed by Kitchenham [42]. We adopt SLR as it is a systematic, comprehensive, structured and repeatable process that is used to identify and analyze published studies [42]. In this study we use SLR to gather information regarding security threats and information security attributes in cloud computing as well as selecting a framework suitable for identifying information security metrics.

4.2.2 Rationale for thorough analysis of the COBIT framework

In this study, we follow the COBIT framework besides other existing security framework such as ISO 27001. This is because the COBIT framework is more focused on business and it aims at ensuring that IT functions enables organizations in meeting strategic and business objectives while reasonably managing IT risks [10]. Since cloud computing is business architecture, we therefore consider the COBIT framework to be more appropriate in the study than other existing security frameworks. Moreover, the COBIT is a measurement-driven framework which provides several metrics to measure IT processes including metrics for measuring SLA and security performance. We will therefore identify metrics from COBIT that can be applicable in cloud computing.

4.3 Research plan

To achieve the objectives, we divide the study into three main phases as described in following subsections and presented in figure 5.

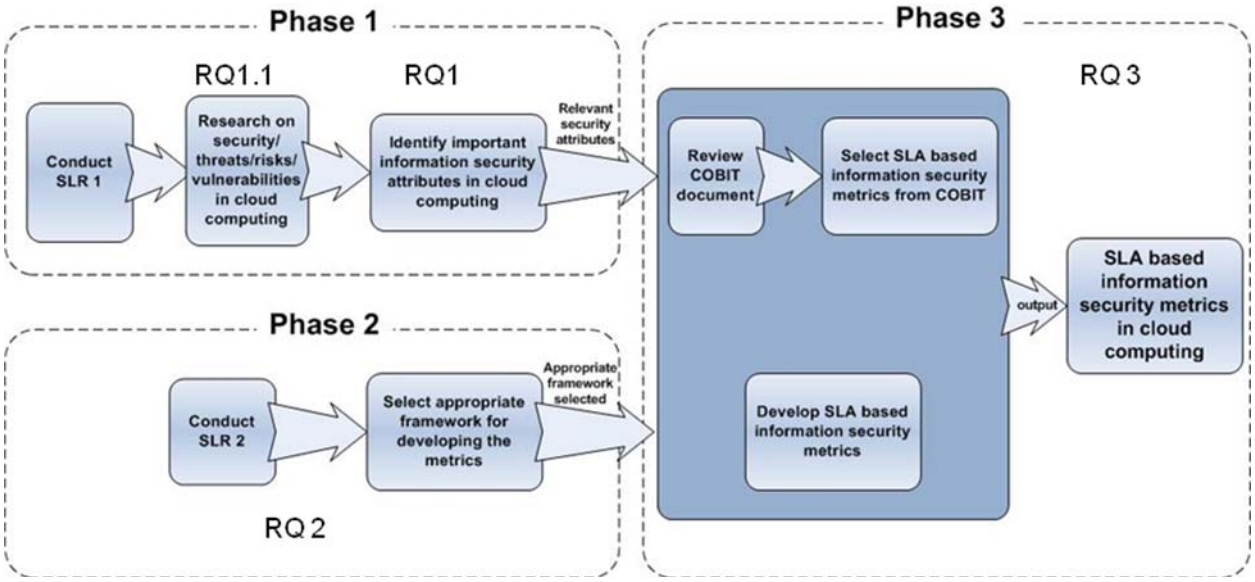

Figure 5: Research plan

4.3.1 Phase 1: Identification of information security threats in cloud computing

Phase 1 corresponds to RQ1 and RQ1.1. The phase aims at collecting data to answer RQ1.1 which is about information security issues, threats or risks in cloud computing. Accordingly, the data for answering RQ1 which is concerned with information security attributes are collected. This is done through SLR in published studies. As suggested by Kitchenham, we set the inclusion/exclusion [42] criteria for the study to be considered in this research work. The defined inclusion/exclusion criteria are presented in table 2.

Table 2: Study inclusion/exclusion criteria for SLR1

Initial filter criteria
The study is peer reviewed, written in English and without duplicates
Second filter criteria
Select study based on relevancy of title, abstract and keyword
Final filter criteria
Availability of full text, related with cloud computing security, threats or vulnerabilities

By identifying information security threats or risks in cloud computing we identify relevant information security attributes that would be affected by the threats.

4.3.2 Study quality assessment for SLR1

To ensure that we only include studies with high quality for SLR1 we develop a study quality assessment criteria presented in Table 3. Each criterion is scored with a "Yes", "Partially" or "No" depending on whether the study meets, partly meets or does not meet the criterion respectively. We perform a study quality assessment to all studies that pass the inclusion/exclusion criteria as presented in Table 2 above.

Table 3: Study quality assessment for SLR1

S/N	Quality Criteria	Yes	Partially	No
1	Whether the study focus on security threats or risks in cloud computing.			
2	Whether security threats are clearly presented.			
3	Whether limitations to the study are clearly mentioned.			

4.3.3 Phase 2: Selection of a suitable security metrics framework

Phase 2 corresponds to RQ2. The phase aims at selecting a suitable security metrics framework. We conduct SLR to collect information on available security measurement frameworks. We also follow the inclusion/exclusion criteria as presented in Table 4. Then from several frameworks found in SLR, we select one appropriate framework for identifying the metrics. Selection of the framework is done to assist us in identifying the metrics suitable in cloud computing. The selection is based on four criteria presented in Table 5:

Table 4: Study inclusion/exclusion criteria for SLR2

Initial filter criteria
The study is peer reviewed, written in English and without duplicates
Second filter criteria
Select study based on relevancy of title, abstract and keywords
Final filter criteria
Availability of full text, related with security measurement frameworks

Table 5: Criteria for selecting a suitable security metric framework

S/N	Criteria
1	Simplicity of the framework
2	Acceptability of the framework (Internationally accepted framework and industry validated framework)
3	Universality of the framework i.e the framework may be applied in several different industries.
4	Intended audience of the resulting metrics (in this case the target audience is the management level)

Each criterion above applies a score from 1 to 5, with a 1 representing the lowest and 5 the highest score. We analyze each identified framework and assign appropriate scores. We then select the framework with the highest accumulated score among all frameworks found.

We rely on our own scoring criteria to select suitable framework because we focus on cloud computing area in which the subject itself is not established. In addition, there are not many organizations that have adopted cloud computing technology.

4.3.4 Study quality assessment for SLR2

We develop study quality assessment criteria to ensure that we only include studies with high qualities. Each criterion is scored with a "Yes", "Partially" or "No" depending on whether the study meets, partly meets or does not meet the criterion respectively. The quality assessment criteria are presented in Table 6. The study quality assessment is performed to all studies that pass the inclusion/exclusion criteria for SLR2 as presented in Table 4.

Table 6: Study quality assessment criteria for SLR2

S/N	Criteria	Yes	Partially	No
1	Whether the study focus on security measurement framework			
2	Whether the framework is clearly presented.			
3	Whether limitations to the study are clearly mentioned			

4.3.5 Study pilot selection

We conduct two pilots on study selection for each phase. The aim of the pilots is to ensure both of us have common understanding on the scope and procedures for selecting appropriate studies. The first twenty (20) studies with full text are selected in each phase. Each of us is required to identify studies that are included/excluded based on our criteria and scope. In order to test the level of agreement between us, we perform a Cohen's Kappa statistical analysis as suggested by Kitchenham [42].

The Cohen's Kappa is defined as follows [43]:

$$Kappa = \frac{(P - P_e))}{(1 - P_e)}$$

P as seen in the formula above is proportion of units where there is agreement and P_e is the proportion of units which would be expected to agree by chance [43]. When there is a perfect agreement between the researchers the value of Kappa is 1 [43].

The computed Cohen's Kappa for SLR1 was 0.6875. The observed value of Kappa 0.687 was interpreted that there were good agreement between us based on Kappa interpretation presented by Blan [43]. Blan [43] presents that values of Kappa in the range of 0.61-0.80 are interpreted that there are good agreement between raters. However, based on brainstorming, we established the source of disagreement to be associated with non strict adherence to agreed procedures. We therefore, agreed to strictly adhere to the defined procedures for inclusion/exclusion of the studies. The pilot data which were used in computing the Cohen's Kappa is presented in appendix E.

For SLR2 the computed Cohen's Kappa was 0.4666. Based on interpretation presented by Blan [43], the value is considered moderate. We established that a high level of disagreement was due to unclear scope between us and not following the steps defined in the inclusion/exclusion criteria. We therefore repeated the pilot exercise on other selected 20 papers. The recomputed Cohen's Koppa was 0.8571 which implied that there was very good agreement between us. The pilot data which was used to recompute the Cohen's Kappa is presented in appendix F.

4.3.6 Phase 3: Data collection for identification of information security metrics

Phase 3 corresponds to RQ3. The phase aims at identifying SLA based information security metrics relevant in cloud computing. This is done through thorough analysis of COBIT framework. Thorough analysis is conducted to gain in-depth knowledge of COBIT framework and be able to identify SLA based information security metrics in cloud computing. Based on the results of phase 2, the selected framework GQM approach is followed to identify SLA based information security metrics in the cloud computing. We

adopt a GQM approach template proposed by Basili et al. [28] as presented in Table 7 to help in identifying the metrics.

Table 7: GQM approach template [28]

Goal	Purpose	
	Issue	
	Object (process)	
	Viewpoint	
Question		
Metric		

The GQM approach is structured into three main sections namely Goal, Question and Metrics [28]. The key parts of the templates are the goal section that comprises purpose of measurement, issue to be measured, object to be measured, and viewpoint from which the measurement is taken. The goal is thereafter refined into several questions and each question is further refined into several metrics [27] [28].

Therefore, we first identify the objects (processes) from COBIT that are related with information security and which are to be measured in cloud computing. For each object we then define purpose, issue, viewpoint, questions and metrics. Based on the COBIT framework alone a massive number of metrics could have been identified. However, to identify only those metrics that are relevant to this study, we apply the criteria as presented in Table 8.

Table 8: Criteria for selecting SLA based information security metrics in cloud computing

S/N	**Criteria**
1	Related with information security
2	Applicable in the SLA for cloud computing
3	Within the cloud provider's control
4	Useful to a certain targeted audience , in this case the targeted audience was the senior managers

This approach helps us to identify a manageable number of metrics that are related with information security and which can be included in the SLA when measuring security issues in the cloud computing environment.

4.4 Sources of data

We conduct SLR on two main electronic reference databases namely Engineering Village and Scopus. We select these databases because they are among the largest abstract and citation databases containing high quality scientific literatures including peer reviewed conference papers, journals as well as web sources. The Engineering Village provided by BTH comprises Inspect and Compendex which are two main comprehensive citation and abstract databases. On the other hand, the Scopus database is also among the largest citation and abstract databases. Scopus has interoperability functionality with other reputable and large electronic databases including SciVerse ScienceDirect, Scirus [44]. Additionally, Scopus contains citation and abstract information of peer reviewed scientific conference papers from proceedings and journals including those published by Cambridge University Press, Elsevier, Springer/Kluwer, the Institute Electronics Engineers (IEEE) [44].

Besides extensive coverage of Engineering Village and Scopus databases, both have very intuitive functionality that makes searching and reference handling easy.

To avoid missing other important studies we also gather information from other security reputable online publications including NIST, SANS, European Network and Information Security Agency (ENISA) and Information Systems Audit and Control Association (ISACA). We also include published studies from these organizations in order to get information that is close to what is happening in the industry. This is because very often these organizations conduct scientific studies that involve industry practitioners.

We consider the selected databases to be sufficiently good to provide us with satisfactory knowledge of literatures on cloud computing. Despite cloud computing being a fairly new and evolving subject, we are able to derive our aim and objectives of this study based on the selected databases.

4.5 Data analysis

We analyze the data gathered in this study as presented hereunder:

4.5.1 SLR1 and identification of information security threats

During SLR1 we collect information on possible security threats in cloud computing. Based on the threats identified we establish relevant information security attributes which are affected by each threat in cloud computing. To maintain consistency and completeness of the collected data, we develop a data extraction form that is used by both of us.

We conduct a pilot data extraction exercise on random ten (10) studies obtained from SLR. The pilot exercise aims at detecting defects in the data extraction form as well as to obtain common understandings of the form between us. The data extraction form is then revised to address observed shortcomings. The final data extraction form is as presented in Table 9.

Table 9: Data extraction form for information security threats and attributes in cloud computing

S/N	Threats	Threat Description	Source	Security Attribute Affected

To minimize biasness and avoid influencing each other, each of us identifies relevant security attributes in cloud computing first. Thereafter, both of us review the individual results together to identify and agree on security attributes relevant in cloud computing.

4.5.2 SLR2 and identification of security metrics frameworks

We conduct a second SLR to collect data on frameworks available for developing security metrics. The collected data include name of framework and its key features/steps. We also collect data on its objectives and area/industry the framework is intended to be used. Similar to SLR1, we conduct a pilot data extraction exercise on random three (3) studies to ascertain completeness of and detect defects in the data extraction form. We use the frameworks data extraction form as presented in Table 10 .

We brainstorm and assign scoring to each security metric framework identified based on framework selection criteria as defined in research plan section (See 4.3). The individual framework scores are recorded in a framework data extraction form presented in Table 10. A framework with the highest accumulated score is selected and used in the following stages of study. Table 10 also presents an example of how the framework data extraction form is used.

Table 10: Data extraction form for security metrics frameworks

S/N	Framework Name	Feature/steps (description of the framework)	Individual framework scores (Mark 1-5 for each criteria)				Accumulated score (sum of individual criteria score)	Remarks
			Simplicity	Acceptability	Universality	Intended Audience		
1	NIST		2	4	1	5	12	

4.5.3 Data analysis for identification of SLA based information security metrics

Based on security attributes identified in cloud computing and the selected framework, we follow the GQM approach template [28] to identify SLA based information security metrics from the COBIT framework. The process of identifying the SLA information security metrics is driven by the goals and the questions that are defined by us following the GQM approach. In case, of those information security metrics that cannot be obtained in COBIT, we identify the metrics based on other sources including the Center for Internet Security (CIS). Based on the adopted GQM metric template [28] we identify the SLA based information security metrics in cloud computing.

We recognize the facts that the COBIT framework is organized into four (4) IT domains which further extends into thirty four (34) IT processes [10]. However, not all of the 34 IT processes are closely related with information security. For instance, the COBIT process PO10 mainly focuses on managing IT projects and the PO5 focuses on managing IT investments. At times these objects maybe useful and relevant in information security, however in this study they are considered not relevant. In identifying the information security metrics we therefore focus on those objects that are related with information security and relevant in the cloud computing. We follow the criteria presented in Table 11. We evaluate the COBIT IT processes based on the simple "Yes" or "No" answers. The "Yes" indicates that the process meets a criterion whereas "No" indicates that the process does not meet a criterion. Only those objects that meet all three criteria are selected and considered for developing information security metrics.

Table 11: Criteria for selecting objects

S/N	Criteria	Yes/No
1	The object is related with information security	
2	The object is relevant in the cloud computing environment	
3	The objects has some tasks that are performed by the cloud provider	

5 RESULTS

In this section, the results of the study are presented. Section 5.1 presents study selection for SLR1, and 5.2 presents study selection for SLR2. The identified relevant security attributes and security metrics framework are presented in section 5.3 and 5.4 respectively. Lastly, section 5.5 presents results of the identified information security metrics.

5.1 Study selection for SLR1

5.1.1 Results for study selection and inclusion/exclusion process for SLR1

To collect relevant data for the study, we conducted SLR in the Engineering Village, Scopus and other electronic databases. We used the following search strings:

- **Engineering Village**: *((($cloud $computing) WN KY) AND (($security OR $threats OR $risk* OR $vulnerabilit) WN KY))*
- **Scopus:** *TITLE-ABS-KEY(((cloud computing) AND ($security OR $threat* OR $risk* OR $vulnerabilit*))) AND PUBYEAR AFT 1969*
- **Other databases (ISACA, NIST, SANS, ENISA):** We used simple search string for the keywords cloud computing, security, risks, vulnerabilities.

We did not restrict the publication year of literatures as we did not have background when exactly cloud computing concept started. We therefore intended to discover as much researches in the area as possible. However, publication year 1969 as seen in search string above is the earliest records of year found in Scopus database.

We applied the initial and second selection criteria as stated in table 2 using the built-in features of databases we used. A total of 1058 studies were identified from those electronic databases as presented in figure 6. By using Endnote [45] the studies were merged and duplicates removed. Since Endnote could not remove all duplicate studies, we manually removed remaining duplicates after which 625 studies remained for further analysis. Detailed results of phase 1 study collection are as presented in figure 6:

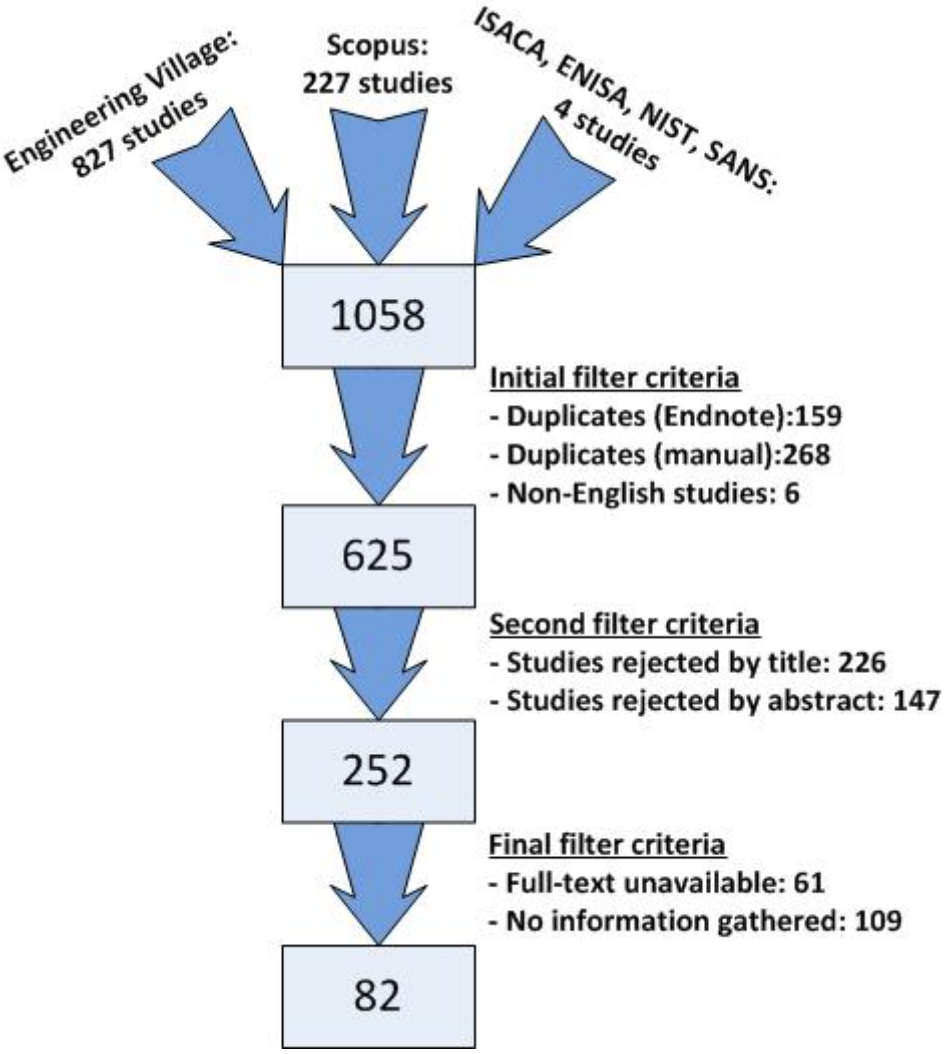

Figure 6: Study collection for SLR1

The 625 studies were distributed between us to identify those studies that are relevant based on the study second filter criteria as stated in table 2. After we applied second filter criteria, it was established that 252 studies were relevant to our study. We then identified that 82 studies are relevant to the study after eliminating 61 non-full text studies and 109 studies that we could not derive the information from.

5.1.2 Results for study quality assessment for SLR1

Table 12 presents results for study quality assessment. Each criterion was scored a "Yes", "Partially" or "No". The result indicates that many studies could not meet second and third criteria as they both recorded 48 and 50 "No" respectively. However, we observe a good number of studies that partially mentioned threats and risks in cloud computing.

Table 12: Summary of studies based on quality assessment criteria for SLR1

S/N	Quality Assessment Criteria	Yes	Partially	No
1	Whether the study focus on security threats or risks in cloud computing.	23	32	27
2	Whether security threats are clearly presented.	13	21	48
3	Whether limitations to the study are clearly mentioned.	18	14	50

5.1.3 Distribution of studies per year of publication

It is observed that out of 82 studies identified, many studies were published in the year of 2000 and later with 2009 recording the highest number of studies as presented in figure 7. The details of the 82 studies together with the year of publications are presented in the appendix G.

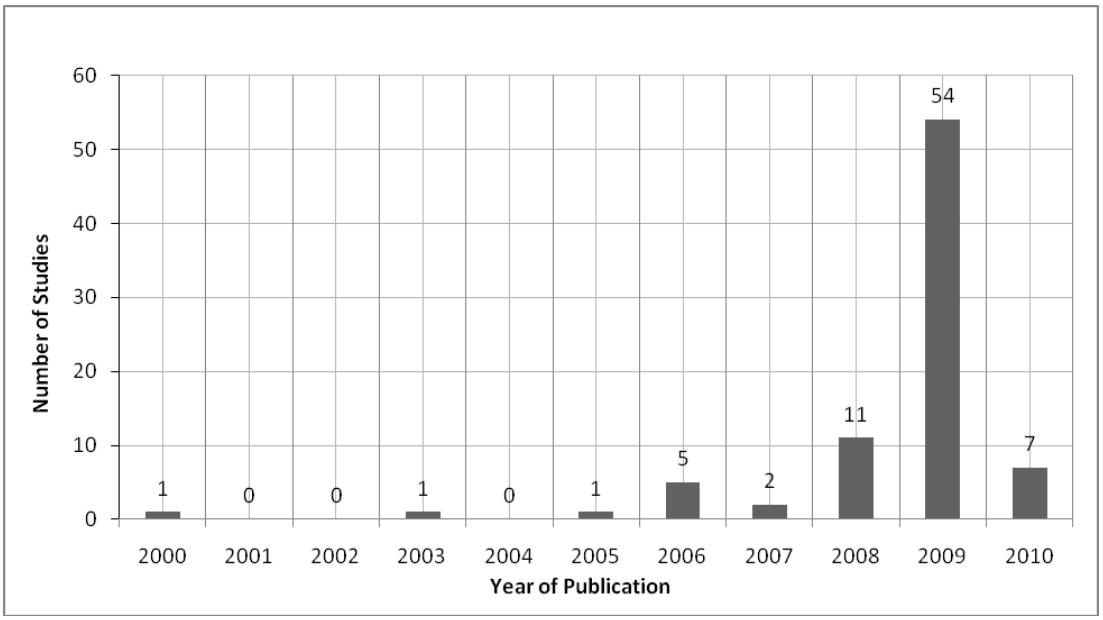

Figure 7: Distribution of studies based on year of publication for SLR 1

5.2 Study selection for SLR2

5.2.1. Results for study selection and inclusion/exclusion process for SLR2

For phase 2, we searched in Engineering Village, Scopus, SANS and NIST electronic databases by using the following search strings:

- **Engineering Village:** *((develop* security metric*) AND((methodolog*) OR (framework*) OR (guideline*)))*
- **Scopus:** *TITLE-ABS-KEY((develop* security metric*) AND((methodolog*) OR (framework*) OR (guideline*)))*
- **Other databases (NIST and SANS):** We used simple search string for the keywords security metric, framework, guidelines and methodology.

We applied the initial and second selection criteria as presented in Table 4 by utilizing the built-in features of the reference database we used. In total, 408 studies were found as presented in figure 8. Likewise, we also used Endnote [45] to merge and remove duplicate studies. We further manually removed duplicates as Endnote could not remove all duplicate studies. 215 papers remained for further analysis after removing duplicates and non-English studies. The detailed results of our search are contained in figure 8.

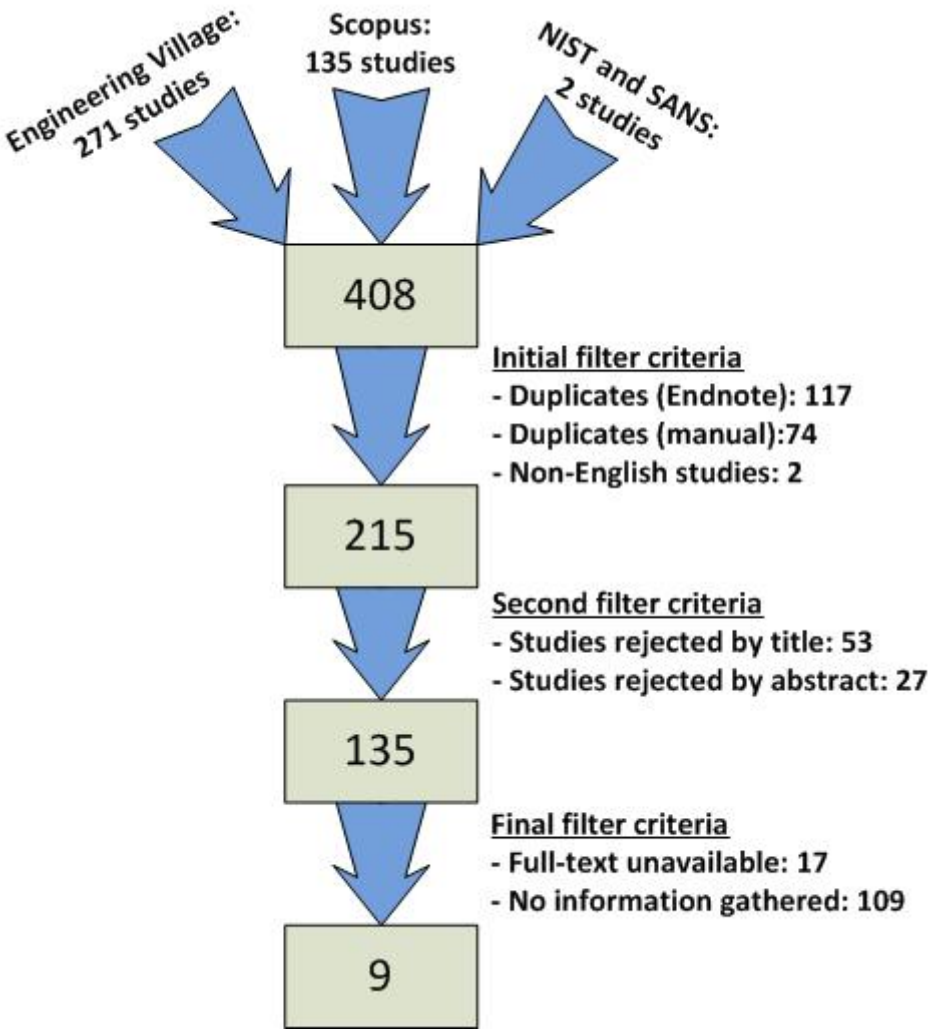

Figure 8: Data collection of SLR2

The 215 studies were distributed between us to determine relevant studies based on final filter criteria defined in Table 4. Nine (9) studies were identified to be relevant to this study after we eliminated 17 non-full text studies and 109 studies that we could not derive the information from. We reviewed the individual analysis results together and reached consensus on the assigned score for each identified framework. The results of the frameworks selection are presented in the result section 5.4.

5.2.2. Results for study quality assessment for SLR2

The relevant studies were assessed to determine if they meet the three assessment criteria we defined. Table 13 presents the results of the quality assessment exercise. The results shows that many studies did not meet the third criterion since 6 studies out of 9 recorded "No". Most probably this is because these studies were industry papers. However, most of the studies were found to meet both the second and third criteria.

Table 13: Summary of studies based on quality assessment criteria for SLR2

S/N	Quality Assessment Criteria	Yes	Partially	No
1	Whether the study focus on security measurement framework	9	0	0
2	Whether the framework is clearly presented.	9	0	0
3	Whether limitations to the study are clearly mentioned	2	1	6

5.3 Identified relevant security attributes

Through analysis twenty two (22) threats were identified in cloud computing as summarized in figure 15 with detailed results presented in appendix A. These threats include unclear ownership and responsibility of data protection, identity theft, data theft, unauthorized modification, malware attacks, denial of service (DOS), lack of data segregation, data inconsistency, inadequate authentication and authorization, unauthorized access, eavesdropping, service disruption, phishing attack, audit difficulty, Insecure Interfaces and APIs, regulatory and legal issues, difficult bugs detection, and difficult intruder (malicious user) detection.

Through brainstorming, we reached consensus on security attributes applicable in cloud computing. These attributes are confidentiality, integrity, availability and accountability. The summary of the results is presented in figure 9 and the details can be found in appendix A. In figure 9, the percentages indicate how each attribute is affected by the threats we identified. For instance, 36% of the identified threats affect confidentiality. These results show that all identified information security attributes are almost of relevancy to the cloud computing.

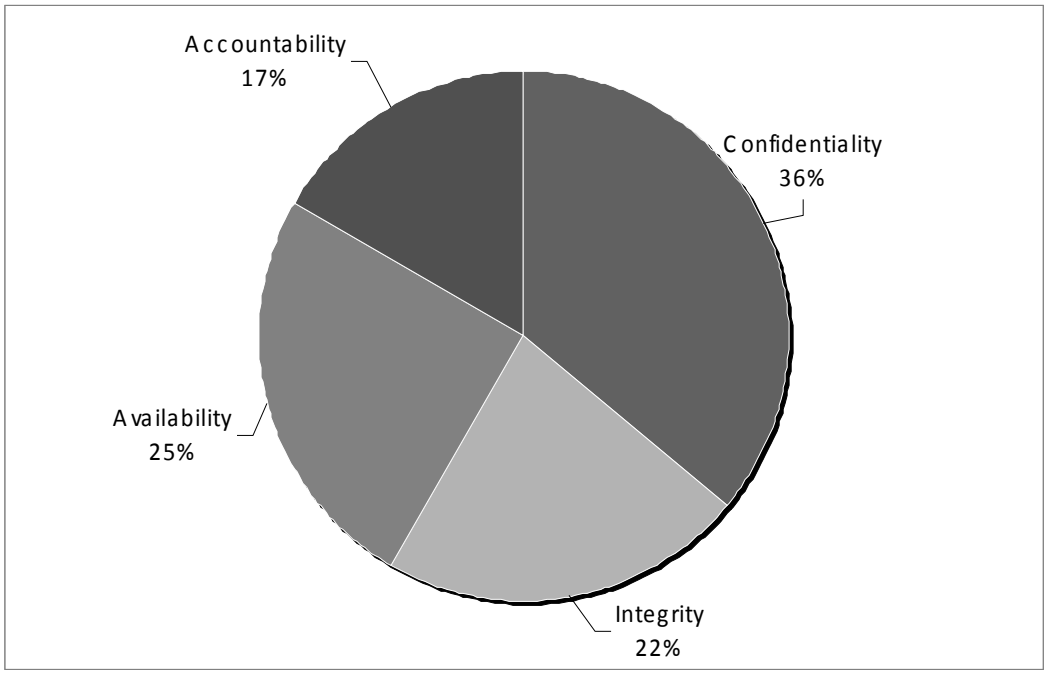

Figure 9: Identified security attributes in cloud computing

5.4 Identified security metric frameworks

In total, eight frameworks were identified. These frameworks are Goal Question Metric (GQM) approach, Framework for policy based metrics, Security Metric Identification Framework, NIST SP800-55, Risk based proactive security COnfiguration manager (ROCONA), Metrics for Electronic bill presentment and payment (EBPP) system, SANS Security metrics guidelines and Security Performance framework. We reviewed the individual data collected together and reached consensus on the assigned score for each identified framework as presented in appendix B. Results summary of the individual criteria score for each framework is presented in figure 10. We summed the individual criteria score to obtain the overall score of each framework which is also detailed in appendix B. The summary of overall score results of each framework is indicated in figure 11. The GQM approach recorded the highest overall score (18 out of 20) of all frameworks identified. We therefore selected the GQM approach to be used in developing the security metrics.

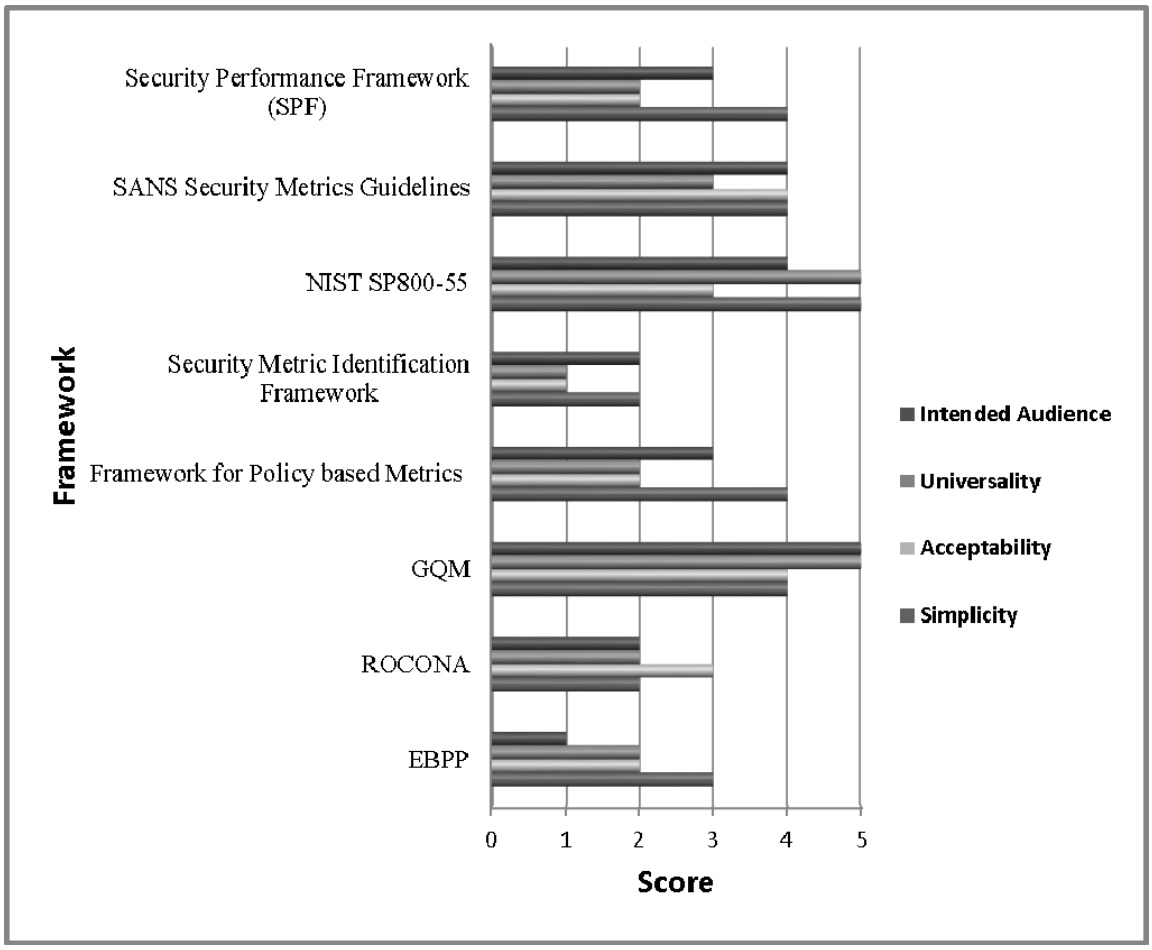

Figure 10: Individual criteria score per framework

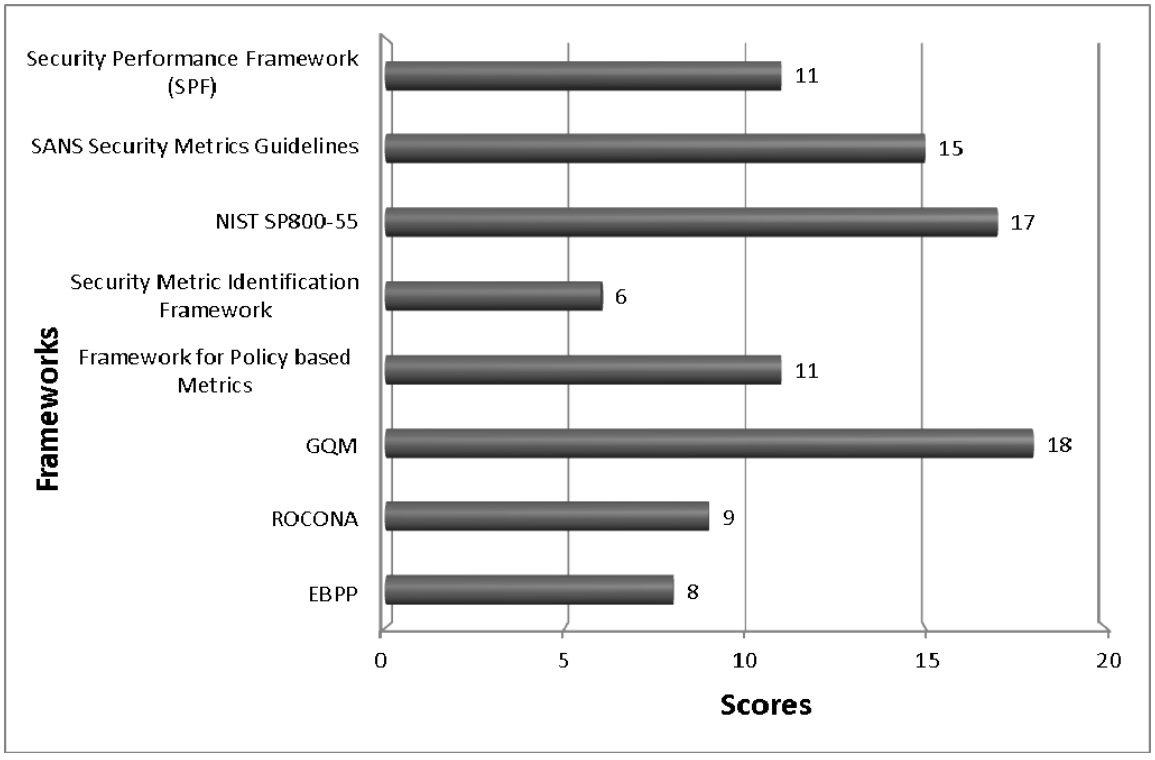

Figure 11: Overall score distribution for each identified frameworks

5.5 Identified information security metrics

We applied criteria for selecting objects as presented in Table 11. We found that fourteen (14) out of 34 COBIT IT processes met the criteria. The COBIT IT processes that met the criteria are as presented in appendix C1. Details of results for the selection of the objects are presented in appendix C2.

We observed that some COBIT IT processes are closely related to each other. Therefore, we combined some IT COBIT processes and renamed them accordingly. After combining and renaming the COBIT IT process that met the criteria, we came out with ten (10) objects as presented in Table 14.

Table 14: Objects relevant in cloud computing

S/N	Object Name
1.	Configuration management
2.	Change management
3.	Problems and incident management
4.	Risk management
5.	Compliance issues
6.	Operations management
7.	Performance and capacity management
8.	Continuity of IT services
9.	IT security management
10.	Software management

We formulated some metric goals for each of the identified objects. We also formulated questions to be answered so that assurance on the achievement of the set goals is obtained. Moreover, some metrics were identified for each redefined questions as presented in appendix D. We formulated a total of 19 questions and identified 41 metrics that are relevant in cloud computing in the viewpoint of senior managers. Results summary of the identified SLA based information security metrics is presented in figure 12.

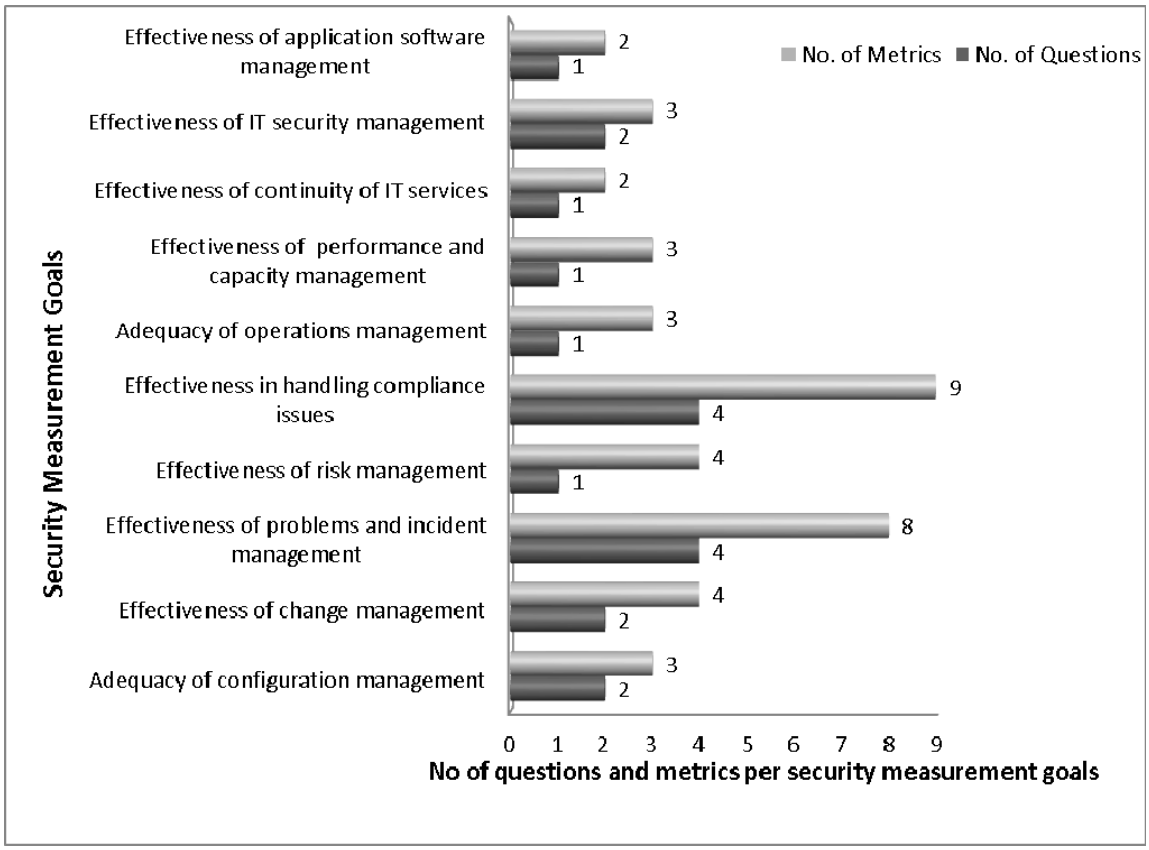

Figure 12: Summary of identified SLA based information security metrics

Figure 13 presents a distribution of metrics in each security measurement goals grouped in accordance to the three types of metrics namely implementation, impact, and effectiveness/efficiency [34]. The highest number of metrics is recorded in the types of impact within the security goal of effectiveness in handling compliance issues. This is followed by metrics in the types of implementation also falling within the security goal of effectiveness in handling compliance issues. The security goal of effectiveness of problems and incident management is the second goal which recorded large number of metrics in the types of impact and effectiveness/efficiency. These results suggest that handling problems, incidents and compliance is critical in cloud computing. However, other objects should also be given appropriate attention depending on the nature of business operations deployed in the cloud and the cloud services adopted.

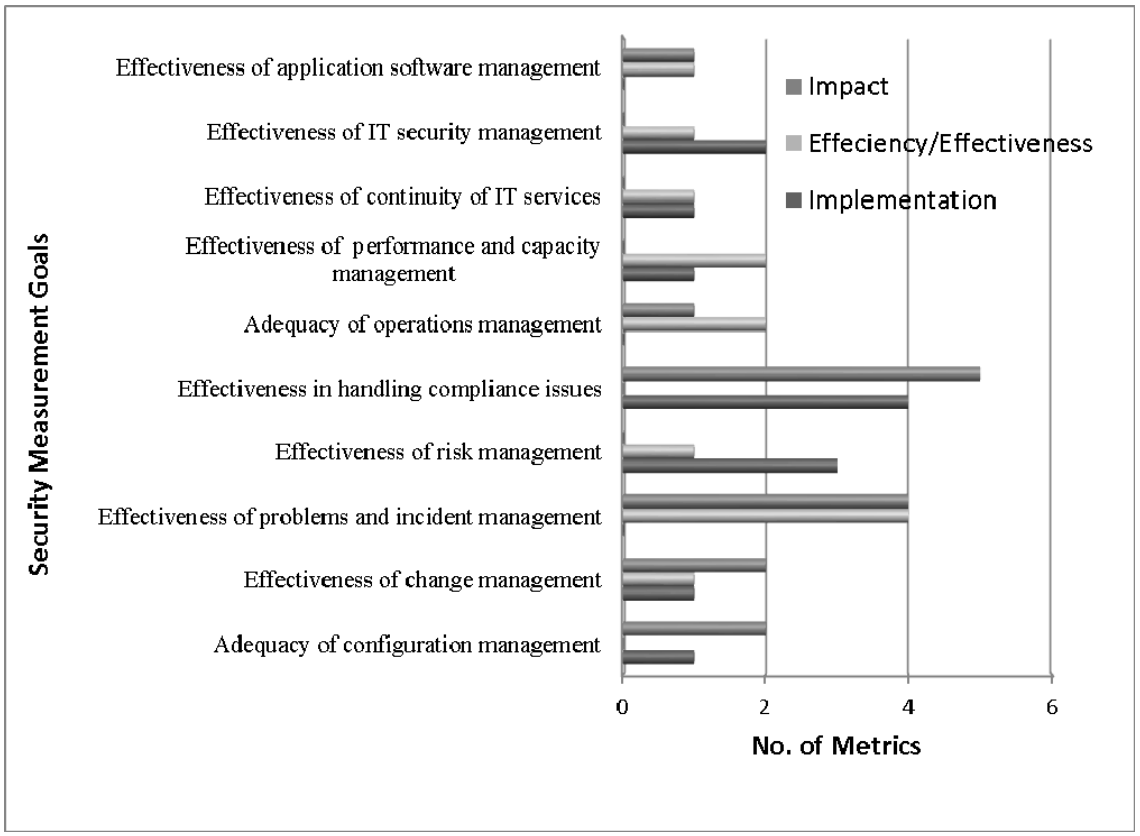

Figure 13: Distribution of types of metrics per security measurement goals

Result summary of the identified metrics per types of metrics is presented in figure 14. The metric type of impact recorded 36% of all the metrics identified. Implementation and effectiveness/efficiency types each recorded 32% whereas implementation type recorded 32%. The results presented in figure 14 suggest that organizations should equally consider the different types of metrics in order to effectively measure information security performance in the cloud.

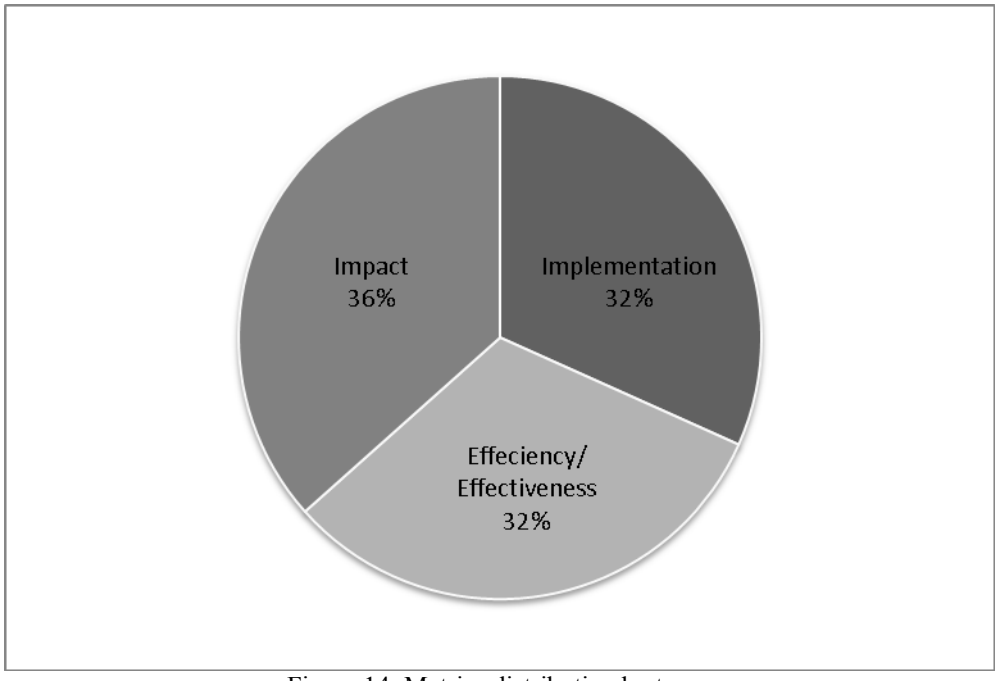

Figure 14: Metrics distribution by types

6 ANALYSIS

This study intends to answer three main research questions and one sub research question. The three research questions are RQ1 (What information security attributes are relevant in cloud computing?), RQ2 (Which framework is suitable for developing security metrics?) and RQ3 (What are SLA based information security metrics in cloud computing?). One sub research question answered is RQ1.1 (What information security threats are relevant in cloud computing?). In this section we describe how the research questions were answered in the study.

6.1 Information security attributes in cloud computing (RQ1)

In traditional computing environment the commonly referred to be information security attributes are confidentiality, integrity and availability [30] [46]. In addition to the three principal security attributes accountability and non-repudiation are also considered [30]. This research question aims at establishing whether the same information security attributes are still applicable in cloud computing which is an emerging technology. As it was difficult to directly obtain these attributes from the literature, we therefore derived them through obtaining answers of RQ1.1. Thus based on information security threats we were able to deduce the security attributes relevant in cloud computing. As presented under the result section 5.3, the study identified confidentiality, integrity, availability and accountability to be the information security attributes in cloud computing.

Among the four attributes, confidentiality appeared to be mostly affected by the threats listed in section 6.2. The details of the threats can be found in appendix A. The results presented in figure 9 indicate that 36% of the identified threats appeared to affect confidentiality. However, it is clear that one threat might affect more than one security attributes as presented in detail in appendix A. For instance, an unauthorized access may lead to compromise of confidentiality, integrity and availability depending on attacker motives and capabilities. Generally, one threat might affect more than one security attributes as presented in detail in appendix A.

6.2 Information security threats in cloud computing (RQ1.1)

Information security threat has been defined by Pfleeger and Pfleeger [46] as anything that can cause harm or loss to a computing environment. Usually threats exploit security weaknesses existing in the computing environment [46]. The authors [46] categorize threats into four classes namely interception, interruption, modification and fabrication [46]. If these threats become actualized the result is a compromise of one or more security attributes which are confidentiality, integrity, availability and accountability. Cloud computing being an emerging technology, we intended to identify threats in such a computing environment through obtaining answers to RQ 1.1.

We observed lack of common vocabulary for the threats among the studies we found. As a result, we avoided listing threats with different names but which in principal meant the same thing. Therefore a threat name of more preference to us was considered. For instance, Cloud Security Alliance (CSA) [47] defines “account or service hijacking” threat in cloud computing to include phishing threat. However, we define phishing as its own threat and differentiate it from account or service hijacking (in this study is referred as unauthorized access).

The twenty two (22) information security threats we identified in this study are as summarized in figure 15 with details indicated in appendix A. We observed that the identified threats maps well onto the four classes of threats facing traditional computing

environments. We discovered that among the 22 threats, insecure data storage, malware attacks, DDOS/DOS attacks, and unauthorized access threats are the top threats discussed by most researchers. Among the several researchers that studied about insecure data storage threat is Henrich et al. [48]. The researchers argue that cloud provider might have full control over the customers' information kept in the storage which can lead to customers privacy violation [48]. For malware attacks threat, Li et al. [49] argue that as a public data center which is commonly accessed through internet browsers, the cloud is very prone to virus, intrusion and malicious attacks targeting the application layer data. In the case of DDoS/DoS threat, Cayirci et al. [50] present that this threat is attractive to attackers due to massive number of customers, huge databases and high number of processes in cloud computing environment. This scenario then attracts attackers to use multiple identities to consume as much cloud resource as possible [50]. For unauthorized access threats, Paquette et al. [51] argue that the physical data storage may be distributed among several servers over several regions which may lead to easy security compromise.

Although other threats featured the least in the studies we found, this does not mean that such threats should be neglected. Among the threats that were least discussed by researchers include data loss, insecure interface and APIs, difficult bugs detection, regulatory and legal issues, difficult intruder detection as well as unclear ownership responsibility of data protection. We believe that some of these threats are specific to the cloud computing and probably more challenging to mitigate.

We recognize that in order for an attack to be successful three factors namely means, motive and opportunity[52] have to be achieved. The motive refers to the fact that the attacker should have an intent to attack the computing resources [52]. Means refers to how the attacker can gain access on the target system and it is especially about the tools and expertise that are in position by the attacker [52]. Lastly, opportunity refers to the fact that in order to successfully attack the target the attacker needs to identify vulnerabilities in the target system [52]. Considering these factors, therefore it is possible that some threats experienced in traditional computing may become harder to materialize in cloud computing. This is because in cloud computing the attacker is likely to encounter different situation to achieve intended objectives. For instance, in some circumstances the attacker may require to have very specialized knowledge and tools to successful attack the target system.

Some of the threats which we consider that might cause more challenges to the attacker in the cloud includes DDoS and physical theft of hardware. DDoS may be considered harder in cloud computing environment because it is expected that it is more cost effective to establish geographically dispersed redundancy computing resources than it would be in traditional computing. In case of theft of hardware, it may also be considered more cost effective to have a physically secured datacenter in cloud computing than it would be in traditional computing. However, it should be clear that we did not investigate these issues deeply to draw a sound conclusion. It should also be noted that whether certain threats are being properly mitigated in cloud computing than in traditional computing will still depend on security soundness of a specific cloud provider in collaboration with customers. We therefore have the opinions that the matter still warrants for future in-depth investigation. Therefore we advise organizations to consider all these threats, prioritize and mitigate those threats that are most likely to affect their outsourced cloud computing services.

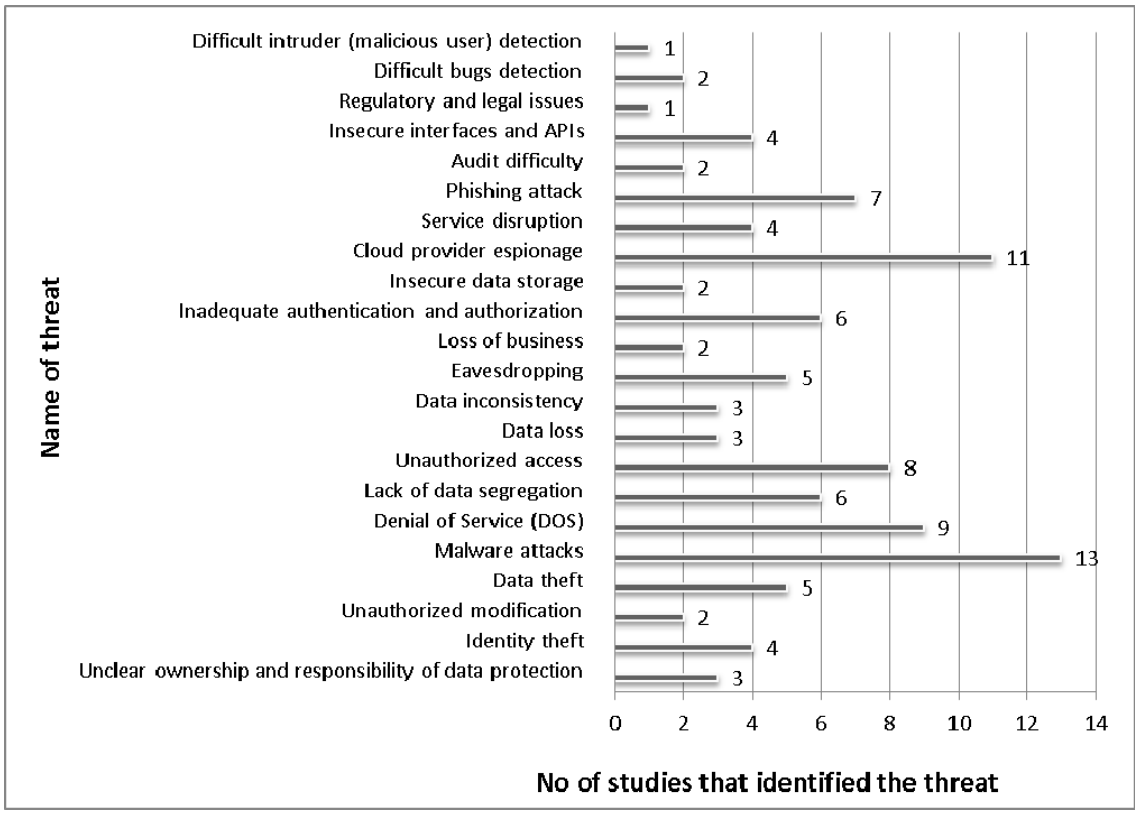

Figure 15: Threats frequencies in the studies

6.3 Frameworks for developing security metrics (RQ2)

As presented in result section 5.4, eight frameworks were identified in this study. The details of each framework along with its brief description are presented in appendix B. The frameworks identified through this study are EBPP, ROCONA, Goal Question Metric, Framework for policy based metrics, security metrics identification framework, NIST SP800-55, SANS security metrics guidelines, and security performance framework.

We recognize that frameworks present simplification of realities. Therefore, as we anticipated, we observed that most of the identified frameworks had some shortcomings. For instance, EBPP [39] and ROCONA [53] frameworks are developed for specific systems. EBPP is intended to measure security level of an electronic bill payment system. Meanwhile, ROCONA [53] is designed to measure proactive security configuration in a network. Moreover, there are no evidences that these frameworks have been validated in the academia or industry. Further, security metric identification framework [54] is newly purposed and it has not been validated. In addition the security metric identification framework [54] was considered too complicated for practical use. The other two frameworks, the framework for policy based metrics and security performance framework mostly relied on organizations policies. Moreover, these two frameworks mostly based on the US NIST guidelines some of which have been superseded. The mentioned shortfalls resulted in those frameworks recording low overall scores when the framework selection criteria were applied.

On the other hand, GQM, NIST SP800-55 and SANS security metrics guidelines were observed to be generic in nature and following a goal based approach in establishing the metrics. All the three frameworks were observed to be simple to use and suitable to produce metrics for the intended audiences of the studies. However, some of the frameworks scored low when the universality criterion was applied. This is due to the facts that some of them have been developed specifically for the US government and might have not been accepted by researchers from other places of the globe such as Europe. Besides, we could not obtain complete documentations for the frameworks especially the SANS security metrics

guidelines. Therefore we feared using such a framework as that might have contributed to wrong results of the study. These shortcomings affected the scoring of each framework. As a result the Goal Question Metrics framework recorded the highest score and was selected to be followed in the next stages of the study.

6.4 SLA based information security metrics in cloud computing (RQ3)

In this study we followed the GQM framework to identify SLA based security metrics in cloud computing. As the GQM is a top-down approach, we initially had clear scope of what security elements need to be considered in the cloud computing and the viewpoint within which the measurement is intended to be used. This argument is supported by Tash and Ghernaouti [38] who suggest that a scope (what to measure) is the primary and first step in undertaking a successful security measurement programme. It is also apparent that without a clear measurement scope organization would end up establishing too many security metrics that are costly and impossible to measure for control and improvements.

As presented in figure 16 in the discussion section, we found that the COBIT framework describes 340 metrics most of which are related with information security. However, we managed to identify only 41 SLA based information security metrics that are relevant in cloud computing in the viewpoint of senior managers. In practice, the identified 41 metrics may still be considered to be many for an organization to adopt and implement. In another study, Villarrubia et al. [55] proposed 22 metrics for Password Management Policy. The 22 metrics might be considered as a huge number of metrics considering the fact that password management is only a minor issue in the broader spectrum of information security area. However, in the scope of their work and depending on their intended audience the 22 security metrics can still be considered to be reasonable. It is therefore suggested that organizations should consider prioritizing and identifying only those metrics they consider to be important in their environment.

We have grouped the metrics we found into three types namely implementation, effectiveness/efficiency and impact as proposed by Chew et al. [34]. The results of this study is in agreement with Tash and Ghernaouti [38] who suggest that a successful security metric programme has to be aligned with business objectives, relevant to the organization and quantifiable. By using the COBIT framework in this study we ensure that our metrics are aligned to the business objectives as COBIT is a business-focused framework.

As part of applying GQM framework, apart from developing metrics we identify ten objects of measurement identified in cloud computing. The identified objects are those that are related with information security based on the criteria presented in Table 11. The descriptions of the ten objects are obtained from COBIT as the main source of data of this study as well as from other relevant studies. The ten objects are described as follows:

i. Configuration management.

It refers to a practice to protect and manage the system and network devices from unauthorized users exploiting the configuration weaknesses [9]. The configuration management deals with managing configuration of IT infrastructure and resources [10]. An effective configuration management facilitates the integrity of software and hardware, provides greater system availability and resolves issues more quickly [10].

ii. Change management.

All changes related to IT infrastructure and applications in cloud computing are supposedly managed in timely and controlled manners [10]. An effective change management will mitigate the risk of negative impacts towards integrity and stability of the cloud system [10].

iii. Problems and incident management.

Information Technology Infrastructure Library (ITIL) [14] defines incident management as restoring services instantly while problem management as identifying and minimizing the root causes of one or multiple similar incidents. In general, problems and incidents managements deal with identification and classification of problems and incidents, root causes analysis, and resolution of problems [10]. Effective problems and incidents management maximize system availability and improve service levels and therefore improve the client's satisfaction [10]. To obtain effective problems and incidents management, it has to be supported with the well-executed service desk [10]. This service desk is intended for clients to register their queries [10].

iv. Risk management.

Risk management covers three processes namely risk assessment, risk mitigation and risk remediation plan. Risk assessment is performed to present to managerial level or stakeholders about the potential financial impact of risks to the organization [10]. Risk mitigation is performed to minimize the impact of potential risks [10]. If any risk takes place and negatively impact the business process, risk remediation plan is performed to restore the business process.

v. Compliance issues.

This process relates to the management and ongoing monitor of compliance with laws, regulations, contractual requirements, internal policies and standards or other requirements [9] [10]. The process involves conducting reviews to ensure obligations are appropriately complied with to reduce occurrence of risks of non-compliance such as fines and public embarrassment [10] [15]. An effective compliance management process prevents the organization's system, application and information from internal and external threats [9].

vi. Operations management.

Operations management includes maintaining operational service of data processing and monitoring IT infrastructure [10]. Effective operations management helps in sustaining data integrity and mitigating errors and failures from IT infrastructure thereby reducing associated IT costs [10].

vii. Performance and capacity management.

Performance and capacity management requires to periodically review current IT performance and resources capacity [10]. This review also involves predicting future storage requirement as the cloud provider should be able to handle customers' demands if they require to increase the storage capacity [9]. An effective performance and capacity management ensures that IT resources that support business needs are constantly available and sufficient now and in the future [10] [15].

viii. Continuity of IT services.

To provide continuous IT services requires developing, maintaining and testing IT continuity plans as well as review backup plans and storage [10]. This process will minimize the probability and impact of critical IT service breakdown [10].

ix. IT Security Management.

Maintaining integrity of information and protecting IT assets require IT security management [10]. This process includes IT security monitoring and periodic testing as well as implementing corrective actions for identified security weaknesses [10]. IT security management also includes the process of establishing IT security roles and responsibilities, policies and procedures [10]. An effective IT security

management protects all IT assets and minimizes the business impacts of security vulnerabilities and incidents [10].

x. *Software management.*

Software management process includes acquiring software that are in line with business requirement [10]. This process should be conducted in timely manner and with reasonable cost [10].

As the responsibilities of cloud provider and customers vary depending on the type of cloud service and deployment model leased, we therefore strongly recommend that appropriate objects should be adopted and mentioned in the SLA.

7 DISCUSSION

7.1 Information security attributes and threats in cloud computing

This study has shown that many studies were published in 2006 and later with the year 2009 recording the largest number of publications as presented in section 5.1.3 figure 7. This suggests that information security in cloud computing environment is gaining more attention from the academia. Further, this suggests that the public community is striving to address information security issues in the cloud which has been among the obstacles for its adoption.

In traditional computing researchers have attempted to identify commonly experienced information security threats or risks. For instance, Pfleeger and Pfleeger [46] present that espionage, organized crime, cyberterrorism, eavesdropping, wiretapping, spoofing, session hijacking and denial of service are among the threats in traditional computing. Pfleeger and Pfleeger [46] argue that information security threats ultimately compromise the security attributes namely confidentiality, integrity and availability.

A recent study conducted by Samy et al. [56] presents 22 threats to health information security. Among the threats identified by [56] include repudiation, social engineering attacks, deliberate acts of theft, willful damages, unauthorized use, and deviations in quality of service.

We observe some commonality when we consider the threats identified in this study as presented in section 6.2 with those presented by Pfleeger and Pfleeger [46] as well as by Samy et al. [56]. This suggests that cloud computing is exposed to the same information security threats as the traditional computing. This conclusion is in agreement with CSA [57] who argues that security controls in the cloud computing are the same as those in traditional computing environment. As CSA further argues that depending on cloud computing model deployed organizations operating in the cloud are likely to face more challenging threats [57].

The results presented in figure 9 identify four information security attributes namely confidentiality, integrity, availability and accountability. Figure 9 further presents that confidentiality, integrity, availability and accountability recorded 36%, 22%, 25% and 17% respectively. These results suggest that of the four attributes identified, confidentiality is considered more important followed by availability, integrity and accountability. Based on these results, it is apparent that the identified attributes are the same as those presented by previous researchers for traditional computing [30] [46]. The fact that non-repudiation was not identified as one of the attributes of information security may be due to lack of common vocabulary in information security as a discipline. This argument maybe considered true as even Pfleeger and Pfleeger [46] do not present non-repudiation as an attribute of information security. In fact Pfleeger and Pfleeger [46] only present three attributes namely confidentiality, integrity and availability. This may also be contributed by the facts that cloud computing is still an immature technology.

Despite this discrepancy, we argue that non-repudiation is among the attributes of information security which is even more important to be considered in cloud computing. This is true because in cloud computing mostly computing resources are managed by the cloud provider whilst the cloud customers still wish to maintain control over the services. In other words parties involved in the cloud should not be in a situation whereby one of them can deny to have participated in committing a certain transaction.

7.2 Selection of GQM framework

As mentioned in section 5.4, the end result of phase 2 (identifying framework for developing metrics) is a suitable security metric framework. The need for identifying a metric framework was necessitated by the facts that numerous metrics have been proposed

implying that it is hard to identify a manageable number of security metrics. This is observed to be true as we found that the COBIT framework [10] describes 340 metrics as indicated in figure 16. Although not all of the metrics presented in the COBIT framework are relevant in cloud computing and specifically SLA related, it is clear that without a proper model for identifying the metrics researchers could have identified a huge number of security metrics. This argument is supported by Basili et al. [28] who point out that without having a proper model and goal definition, it may not be clear on what metrics to use and how those metrics have to be interpreted .

We identified eight (8) frameworks as presented in the results section 5.4. Each of the identified frameworks has its own shortcomings. Studies have also shown that bottom-up framework may not produce better metrics as there exists too many object characteristics to observe [28]. We observed that NIST SP800-55 [34], SANS security metrics guidelines [40] and GQM [26] [28] all are considered to be based on top-down approach. However, when we applied the metric frameworks selection criteria some of the framework scored low especially in the acceptability and universality criteria.

We therefore selected the GQM framework for developing the metrics because it has the highest score when four criteria (simplicity, acceptability, universality, intended use) are applied. Further, besides having the highest score GQM is top-down measurement in which it starts from goal (conceptual level) going down to questions (operational level) and metrics (quantitative level). Therefore, GQM helped us to have a clear scope when we select SLA based information security metrics that are relevant in cloud computing.

7.3 SLA based information security metrics

In this study, we identify SLA based information security metrics that can be used by cloud customer to measure information security performance of the cloud services. Although organizations may use in their cloud environment all of the metrics presented in this study as is, a better understanding of their environment is of paramount. In understanding their cloud environment organization may consider such issues as the type of cloud services and cloud deployment model adopted. Other issues may include regulatory issues governing their business and industry.

Tashi and Ghernaouti [38] suggest that a scope (what to measure) is the primary and first step in undertaking a successful security measurement programme. It is also apparent that without a clear measurement scope organization would end up identifying too many security metrics that are costly and impossible to measure for control and improvements. In this study we focus on ten objects that we consider to be more important in the cloud environment. These objects and their descriptions are presented in section 6.4. The objects were identified based on the COBIT framework. However, we see that these objects are closely related with the issues CSA [47] considers as critical areas in cloud computing. The areas that CSA [47] considers critical include compliance and audit, information lifecycle management, traditional security, business continuity, and disaster recovery, incident response, notification, and remediation, application security, identity and access management. Therefore we argue that the objects we identified in this study for SLA measurement respond to the business need in addressing information security issues in the cloud computing.

While we identify the metrics we had in mind the characteristics of a good metric as suggested by Jaquith [31] . The suggested characteristics are that the metrics should be consistently measured, cheap to gather, expressed as a cardinal number or percentage , expressed using at least one unit of measure and contextually specific. The metrics presented in this study are in viewpoint of the decision makers so that they can timely take appropriate actions regarding their services in the cloud computing. We also considered the five principles of selecting SLA metrics as suggested by Hayes [4]. The suggested principles are that SLA metrics have to motivate the right behaviour (meet expectation and goals of the customer), reflect factors within the provider's control, easily gathered, not too excessive number of metrics and that set reasonable attainable performance levels.

As shown in figure 16, we observed that a single COBIT domain of Deliver and Support (DS) has 120 metrics which is 35% when compared with a total of 340 metrics presented in the COBIT framework. Such a huge number of metrics as observed in the COBIT framework or a single DS domain may be costly to implement. It may also become merely impossible for an organization to successfully collect the data and measure their information security processes for control and improvement purposes. Moreover, it may not be consistent with the five SLA principles suggested by Hayes [4].

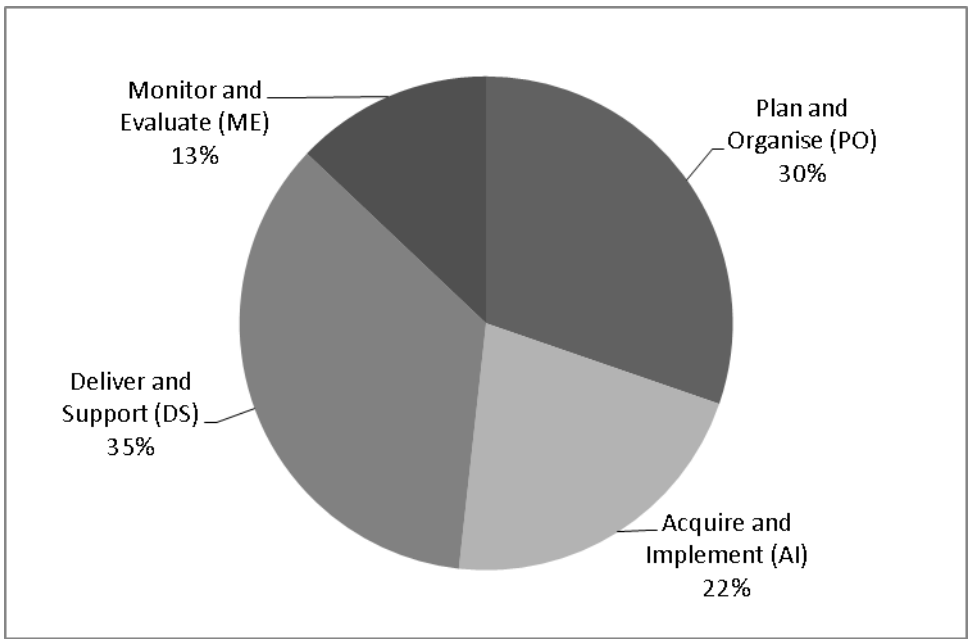

Figure 16: Distribution of metrics in the four domains of COBIT

We followed the GQM framework and identified only 41 SLA based information security metrics for cloud computing. These 41 metrics are about 12% when compared with the 340 metrics presented in the COBIT framework.

The facts that we identify SLA based information security metrics in cloud computing implies that we solve a problem relevant to organizations as the importance of SLA, security and cloud computing is today becoming a major concern to the business. The reasonable number of metrics we identified in this study suggests that organization will be able to inexpensively, continuously and repeatedly measure cloud security performance and justify their spending.

We therefore believe that cloud computing customers and providers can prioritize and adopt the information security metrics presented in this study. Successful execution of cloud computing SLAs that consider information security metrics will likely improve security in the cloud.

8 VALIDITY RISKS

Validity risks or commonly known as validity threats concern with how valid the results of a study are [58]. In this study we use validity risks instead of validity threats to avoid confusion with the term “threat” used in this study.

To answer research questions stated, this study solely based on literature identified in several databases such as Engineering Village and Scopus. The identified literatures were analyzed particularly to identify information security attributes in cloud computing. Moreover we selected a framework for identifying information security metrics from literatures. However, by relying on databases mentioned we could have missed some important studies. To mitigate this risk, we covered several security specific organizations sites such as NIST, SANS, and ISACA that are known to contribute on security related issues and their researches are close to the industry practices.

When conducting the first SLR (SLR1) we anticipated two validity risks. The first risk was that the study was performed by two of us hence we could have faced the problem of maintaining consistency and completeness of the collected data. We mitigated this risk by developing data collection form. The data extraction form also helped us in resolving conflicts encountered during the data extraction process. In addition, we anticipated that the data collection form might have some defects that could have affected the results. We mitigated this risk by performing a pilot data extraction exercise to detect and fix form defects.

During the second SLR (SLR2) we anticipated the risk of selecting a metric framework that might have not been suitable to this study. We addressed the risk by developing selection criteria that were rigorously applied. Moreover, each of us applied the selection criteria individually. Both of us then reviewed the individual results to come up with a suitable framework. This approach reduced biasness between us and helped in resolving conflicts when disagreement arose. We appreciate the fact that the sample size of two of us applying the criteria may not be sufficient to conclude that the selected framework is suitable in practical sense. However, considering that cloud computing is still immature it is considered difficult to obtain reasonable sample size of industry practitioners well-versed in the area who could have helped us in scoring the criteria.

Another risk that we anticipated is that the selected framework might not be applicable in all industries. We addressed the threat by establishing universality criteria in which we intended to verify whether the frameworks found in the literature could be applicable in all industries in every part of the world. In addition, we appreciate the fact that to have our results generalized to all industries we were supposed to interact with large population sample across various industries.

We also appreciate the fact that our results might not be generalized to different cloud computing services such as IaaS, PaaS as well as SaaS because we focused on cloud computing in general. This might also be the case for the different cloud computing deployment models which are private, community, public and hybrid. We propose the work to consider the different services and model in the future.

9 CONCLUSION AND FUTURE WORK

Cloud computing is an emerging and growing subject in IT industry. Many organizations are exploring cloud computing as a prospering cost effective computing option for their enterprise needs. Some organizations have already entrusted their sensitive information to be stored in cloud computing environment. Besides that there are a number of issues that hinders adoption of cloud computing. Among these issues are security, privacy issues, lack of standard for measuring the SLA, complexity in adherence to compliance and audit, regulatory and legal issues as the data might be processed and stored beyond the cloud customer boundaries. This study has addressed the issue of improving information security in the cloud using SLA metrics.

It has been revealed in this study that cloud computing is exposed to the same threats as those facing traditional computing environment. Due to the nature of cloud computing service delivery and deployment models, cloud customers become exposed to more challenging security threats and risks than the traditional computing counterparty. As it has been established in this study, cloud providers have key responsibilities for creating not only a cost effective but also a secure cloud computing service.

Many researchers have suggested that SLA may be used by both cloud customers and providers as a tool for establishing common expectations and goals. For instance, ISACA [59] suggests that SLA is an effective tool to address cloud computing risks. In this study we therefore assist both cloud provider and customers on the security issues that we believe are to be considered for inclusion in their SLA. We further help them with a number of SLA based information security metrics that might be considered in measuring whether the anticipated security performance and goals of the cloud services are being met.

The SLA based information security metrics identified in this study are generic. The metrics are intended for all cloud computing services and deployment models. Because of time constraint, it is not possible for us to study the metrics to be applicable specifically for each cloud computing type of service and deployment model.

We have learnt that electronic citation databases works based on semantic analysis. However, overtime concepts especially in technology changes. Therefore, researchers need to be aware of these changes in order to obtain reliable search results.

We found that the security in cloud computing architecture is challenging as the subject of cloud computing itself is still developing and evolving. Considering the case of Europe, cloud computing is emerging in the region. This situation has necessitated us to obtain information of this study only based on systematic literature review of published academic studies. Nevertheless we believe cloud computing gains attention from IT professionals in industry now and even much more in the future. Several researchers also believe that cloud computing will be widely integrated in the industry. In spite of immature state of cloud computing, the study identified SLA based information security metrics in cloud computing environment as the end results. As a potential future work we can demonstrate the output of this study in academia or industry for validation.

10 REFERENCES

[1] K. Jeffery, and B. Neidecker-Lutz, The Future of Cloud Computing Opportunities for European Cloud Computing Beyond 2010, European Commission Information Society and Media.

[2] R. Barga, J. Bernabeu-Auban, D. Gannon et al., “Cloud computing architecture and application programming,” SIGACT News, vol. 40, no. 2, pp. 94-5, 2009.

[3] B. R. Kandukuri, V. R. Paturi, and A. Rakshit, "Cloud security issues," 2009 IEEE International Conference on Services Computing (SCC). pp. 517-20.

[4] S. I. Hayes, "Metrics for IT outsourcing Service Level Agreements," http://www.clarity-consulting.com/MetricsforIToutsourcing.pdf, 2004].

[5] GoGrid, "GoGrid Service Level Agreement (SLA)," http://www.gogrid.com/legal/sla.php, [August 10, 2010, 2010].

[6] R. Clarke, "User Requirements for Cloud Computing Architecture," Proceedings 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGrid). pp. 625-30.

[7] D. Winder, “What's in store for 2010?,” Infosecurity, vol. 7, no. 1, pp. 10-15, 2010.

[8] M. Peter, and G. Tim. "The NIST Definition of Cloud Computing," 19 June, 2010.

[9] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy An Enterprise Perspective on Risks and Compliance: O'Reilly, 2009.

[10] I. G. Institute, "COBIT 4.1," 2007.

[11] CIS, "The CIS Security Metrics v1.0.0," https://www.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.0.0.pdf, [May 2010, 2009].

[12] R. Kissel, "Glossary of Key Information Security Terms ", NIST, 2006.

[13] F. Cuijiao, “Research of Security Vulnerability in the Computer Network ” in IEEE, 2010.

[14] ITIL. "ITIL Open Guide," 20 July 2010; http://www.itlibrary.org.

[15] Enisa, Cloud Computing Benefits, risks and recommendations for information security, 2009.

[16] M. Pokharel, Y. YoungHyun, and P. Jong Sou, "Cloud computing in system architecture," Proceedings of the 2009 International Symposium on Computer Network and Multimedia Technology (CNMT 2009). pp. 5 pp.-5 pp.

[17] R. J. W., and R. J. F., Cloud Computing Implementation, Management, and Security: CRC Press, 2010.

[18] I. Sun Microsystems, Introduction to Cloud Computing Architecture, June 2009.

[19] S. A. de Chaves, C. B. Westphall, and F. R. Lamin, "SLA Perspective in Security Management for Cloud Computing," 2010 Sixth International Conference on Networking and Services (ICNS). pp. 212-17.

[20] B. P. Rimal, C. Eunmi, and I. Lumb, "A taxonomy and survey of cloud computing systems," Proceedings of the 2009 Fifth International Joint Conference on INC, IMS and IDC. pp. 44-51.

[21] G. Institute, COBIT Mapping: Mapping ISO/IEC 17799 :2000 With COBIT, 2006.

[22] G. Institute, COBIT Security Baseline: An Information Survival Kit, 2007.

[23] B. Tuttle, and S. Vandervelde, “An empirical examination of CobiT as an internal control framework for information technology ” International Journal of Accounting Information Systems vol. 8, pp. 240-63, Dec. 2007,.

[24] L. E. Sánchez, D. Villafranca, E. Fernández-Medina et al., "Management of scorecards and metrics to manage security in SMEs." pp. 9-16.

[25] B. v. Solms, “Information Security governance: COBIT or ISO 17799 or both? ,” Computers & Security, vol. 24, pp. 99-104, Mar. 2005.

[26] M. L. Linda, and C. B. M., Software Measurement and Estimation: A Practical Approach: Wiley Interscience, 2006.

[27] v. S. Rini, and B. Egon, The Goal/Question/Metric Method: A Practical Guide for Quality Improvement of Software Development: McGraw-Hill International, 1999.
[28] V. R. Basili, G. Caldiera, and H. D. Rombach, "The Goal Question Metric Approach."
[29] SANS. "SANS Information Security Resources," 18 May 2010; http://www.sans.org/information_security.php.
[30] J. H. Allen, S. Barnum, R. J. Ellison et al., Software Security Engineering: A Guide for Project Managers: Addison Wesley Professional, 2008.
[31] J. Andrew, Security Metrics Replacing Fear, Uncertainty, and Doubt: Addison Wesley, 2007.
[32] W. Jansen, "Directions in Security Metrics Research,NISTIR 7564," NIST, 2009.
[33] K. Erkan, “Evaluating IT Security Performance with Quantifiable Metrics ”, Institutionen f¨or Data- och Systemvetenskap, KTH.
[34] E. Chew, M. Swanson, K. Stine et al., "Performance Measurement Guide for Information Security," NIST Special Publication 800-55 Revision 1, National Institute of Standards and Technology & U.S. Department of Commerce, 2008.
[35] Ł. Skitał, M. Janusz, R. Słota et al., "Service level agreement metrics for real-time application on the grid," 2008, pp. 798-806.
[36] G. Jain, D. Singh, and S. Verma, “Service level agreements in IP networks,” Information Management & Computer Security, vol. 10, no. Copyright 2002, IEE, pp. 171-7, 2002.
[37] V. Stantchev, "Performance evaluation of cloud computing offerings," Proceedings of the 2009 Third International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP 2009). pp. 187-92.
[38] I. Tashi, and S. Ghernaouti, “Efficient Security Measurements and Metrics for Risk Assessment,” in The Third International Conference on Internet Monitoring and Protection, 2008.
[39] H. R. Rao, G. B. Tanna, M. Gupta et al., “Information assurance metric development framework for electronic bill presentment and payment systems using transaction and workflow analysis,” Decision Support Systems, vol. 41, no. Copyright 2006, IEE, pp. 242-61, 2005.
[40] S. C. Payne, "A Guide to Security Metrics," http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55, 2006].
[41] R. Savola, "Towards a security metrics taxonomy for the information and communication technology industry," 2007 International Conference on Software Engineering Advances. pp. 376-82.
[42] B. Kitchenham, Procedures for PerformingSystematic Reviews, Keele University and National ICT Australia Ltd, 2004.
[43] J. M. Blan, "Measuring Health and Disease Cohen’s Kappa - Percentage agreement: a misleading approach," University of York Department of Health Sciences, 2008.
[44] B. V. Elsevier, "SciVerse Scopus Facts & Figures," January 2011, 2010].
[45] EndNote. "endnote reference management tool," http://www.endnoteweb.com/enwebabout.asp.
[46] C. P. Pfleeger, and S. L. Pfleeger, Security in Computing: Prentice Hall, 2006.
[47] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," Cloud Security Alliance, 2009.
[48] C. Henrich, M. Huber, C. Kempka et al., "Brief announcement: Towards secure cloud computing," 2009, pp. 785-786.
[49] L. Yang, L. Zheng, Y. Nenghai et al., "APFA: Asynchronous Parallel Finite Automaton for Deep Packet Inspection in Cloud Computing," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 529-40.
[50] E. Cayirci, R. Chunming, W. Huiskamp et al., "Snow Leopard Cloud: A Multi-national Education Training and Experimentation Cloud and Its Security

Challenges," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 57-68.
[51] S. Paquette, P. T. Jaeger, and S. C. Wilson, “Identifying the security risks associated with governmental use of cloud computing,” Government Information Quarterly, vol. 27, no. 3, pp. 245-253, 2010.
[52] R. A. Caralli, J. F. Stevens, L. R. Young et al., Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process CMU/SEI-2007-TR-012, Carnegie Mellon University, 2007.
[53] E. Al-Shaert, L. Khan, and M. S. Ahmed, "A comprehensive objective network security metric framework for proactive security configuration," CSIIRW'08 - 4th Annual Cyber Security and Information Intelligence Research Workshop: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead.
[54] S. Chandra, and R. A. Khan, "Software security metric identification framework (SSM)," Proceedings of the International Conference on Advances in Computing, Communication and Control, ICAC3'09. pp. 725-731.
[55] C. Villarrubia, E. Fernandez-Medina, and M. Piattini, "Metrics of password management policy," Computational Science and its Applications-ICCSA 2006. International Conference. Proceedings (Lecture Notes in Computer Science Vol.3982). pp. 1013-23.
[56] G. N. Samy, R. Ahmad, and Z. Ismail, "Threats to health information security," 2009 Fifth International Conference on Information Assurance and Security (IAS). pp. 540-3.
[57] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing," 2.1, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, [April 10, 2010, 2009].
[58] W. Claes, R. Per, and H. Martin, Experimentation in Software Engineering An Introduction: Khluwer Academic Pucblishers, 2000.
[59] ISACA, "Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives," http://www.isaca.org/Knowledge-Center/Research/Documents/Cloud-Computing-28Oct09-Research.pdf, [May, 2010, 2009].
[60] F. Jun, C. Yu, and L. Pu, "Bridging the missing link of cloud data storage security in AWS," 2010 7th IEEE Consumer Communications and Networking Conference (CCNC). pp. 2 pp.-2 pp.
[61] M. Jensen, J. Schwenk, N. Gruschka et al., "On technical security issues in cloud computing." pp. 109-116.
[62] S. Pearson, and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 131-44.
[63] H. Xin, Z. Tingting, and H. Yifan, "ID management among clouds." pp. 237-241.
[64] A. Cavoukian, and M. Chibba, "Advancing privacy and security in computing, networking and systems innovations through privacy by design." pp. 358-360.
[65] N. Hawthorn, “Finding security in the cloud,” Computer Fraud and Security, vol. 2009, no. 10, pp. 19-20, 2009.
[66] E. Diaz-Fernandez, M. Ochoa-Fuentes, D. Prieto-Marques et al., “Security 2.0: Facing up to the Tsunami,” UPGRADE: The European Journal for the Informatics Professional, vol. 11, no. 3, pp. 40-5, 2010.
[67] J. Wei, X. Zhang, G. Ammons et al., "Managing security of virtual machine images in a cloud environment," Proceedings of the ACM Conference on Computer and Communications Security. pp. 91-96.
[68] S. Pearson, and A. Charlesworth, "Accountability as a way forward for privacy protection in the cloud," 2009, pp. 131-144.
[69] A. Joint, E. Baker, and E. Eccles, “Hey, you, get off of that cloud?,” Computer Law and Security Report, vol. 25, no. 3, pp. 270-274, 2009.

[70] A. Joint, E. Baker, and E. Eccles, “Hey, you, get off of that cloud?,” Computer Law and Security Report, vol. 25, no. 3, pp. 270-4, 2009.
[71] M. Mowbray, S. Pearson, and Y. Shen, “Enhancing privacy in cloud computing via policy-based obfuscation,” Journal of Supercomputing, pp. 1-25, 2010.
[72] M. Atighetchi, and P. Pal, "From auto-adaptive to survivable and self-regenerative systems - successes, challenges, and future." pp. 98-101.
[73] Y. Li, Z. Li, N. Yu et al., "APFA: Asynchronous parallel finite automaton for deep packet inspection in cloud computing," 2009, pp. 529-540.
[74] W. Qu, M. Li, and C. Weng, "An active trusted model for virtual machine systems." pp. 145-152.
[75] G. Cheng, H. Jin, D. Zou et al., "Building dynamic integrity protection for multiple independent authorities in virtualization-based infrastructure." pp. 113-119.
[76] M. Christodorescu, R. Sailer, D. L. Schales et al., "Cloud security is not (just) virtualization security: A short paper," Proceedings of the ACM Conference on Computer and Communications Security. pp. 97-102.
[77] S. Roschke, C. Feng, and C. Meinel, "Intrusion detection in the cloud," Proceedings of the 2009 International Conference on Dependable, Autonomic and Secure Computing (DASC 2009). pp. 729-34.
[78] W. Huang, and J. Yang, "New network security based on cloud computing." pp. 604-609.
[79] K. Takayama, and H. Yokota, "Performance and reliability of a revocation method utilizing encrypted backup data," Proceedings of the 2009 15th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2009). pp. 151-8.
[80] F. Lombardi, and R. Di Pietro, “Secure virtualization for cloud computing,” Journal of Network and Computer Applications.
[81] T. Jia, and X. Wang, "The construction and realization of the intelligent NIPS based on the cloud security." pp. 1885-1888.
[82] J. Du, W. Wei, X. Gu et al., "Towards secure dataflow processing in open distributed systems." pp. 67-72.
[83] L. Wenjuan, and P. Lingdi, "Trust Model to Enhance Security and Interoperability of Cloud Environment," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 69-79.
[84] S. Mansfield-Devine, “Danger in the clouds,” Network Security, vol. 2008, no. 12, pp. 9-11, 2008.
[85] A. Rosenthal, P. Mork, M. H. Li et al., “Cloud computing: A new business paradigm for biomedical information sharing,” Journal of Biomedical Informatics, vol. 43, no. 2, pp. 342-353, 2010.
[86] I. Muttik, and C. Barton, “Cloud security technologies,” Information Security Technical Report, vol. 14, no. 1, pp. 1-6, 2009.
[87] D. Owens, “Securing elasticity in the cloud: Elastic computing has great potential, but many security challenges remain,” Queue, vol. 8, no. 5, pp. 1-7, 2010.
[88] A. Bakshi, and B. Yogesh, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," Proceedings of the Second International Conference on Communication Software and Networks (ICCSN 2010). pp. 260-4.
[89] T. Jaeger, and J. Schiffman, “Outlook: Cloudy with a chance of security challenges and improvements,” IEEE Security and Privacy, vol. 8, no. 1, pp. 77-80, 2010.
[90] S. Gadia, “Cloud Computing: An Auditor’s Perspective,” ISACA, vol. 6, 2009.
[91] L. Qin, W. Guojun, and W. Jie, "An efficient privacy preserving keyword search scheme in cloud computing," 2009 International Conference on Computational Science and Engineering (CSE). pp. 715-20.
[92] T. Jaeger, and J. Schiffman, “Outlook: cloudy with a chance of security challenges and improvements,” IEEE Security & Privacy, vol. 8, no. 1, pp. 77-80, 2010.
[93] L. M. Kaufman, “Can a trusted environment provide security?,” IEEE Security & Privacy, vol. 8, no. 1, pp. 50-2, 2010.

[94] R. L. Grossman, “The case for cloud computing,” IT Professional, vol. 11, no. 2, pp. 23-27, 2009.
[95] S. Pearson, S. Yun, and M. Mowbray, "A Privacy Manager for Cloud Computing," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 90-106.
[96] N. D. Kho, “Content in the cloud [cloud computing],” EContent, vol. 32, no. 2, pp. 26-30, 2009.
[97] X. Sheng, and G. Weibo, "Mobility Can Help: protect User Identity with Dynamic Credential," Proceedings 11th International Conference on Mobile Data Management (MDM 2010). pp. 378-80.
[98] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a service: privacy-aware data storage and processing in cloud computing architectures," Proceedings of the 2009 International Conference on Dependable, Autonomic and Secure Computing (DASC 2009). pp. 711-16.
[99] W. Jian, Z. Yan, J. Shuo et al., "Providing privacy preserving in cloud computing," 2009 International Conference on Test and Measurement (ICTM 2009). pp. 213-16.
[100] D. Chen, X. Huang, and X. Ren, "Access Control of Cloud Service Based on UCON," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 559-64.
[101] X. Jin-Song, H. Ru-Cheng, H. Wan-Ming et al., "Secure Document Service for Cloud Computing," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 541-6.
[102] V. Raval, “Risk Landscape of Cloud Computing,” ISACA, vol. 1, 2010.
[103] Z. Shuai, Z. Shufen, C. Xuebin et al., "Cloud Computing Research and Development Trend," 2010 Second International Conference on Future Networks (ICFN 2010). pp. 93-7.
[104] Q. Wang, C. Wang, J. Li et al., "Enabling public verifiability and data dynamics for storage security in cloud computing," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 355-370.
[105] W. Cong, W. Qian, R. Kui et al., "Ensuring data storage security in cloud computing," 2009 IEEE 17th International Workshop on Quality of Service (IWQoS). pp. 9 pp.-9 pp.
[106] W. Vogels, “Eventually Consistent [distributed systems],” ACM Queue, vol. 6, no. 6, pp. 6 pp.-6 pp., 2008.
[107] M. S. Blumenthal, “Hide and Seek in the Cloud [security in cloud computing],” IEEE Security & Privacy, vol. 8, no. 2, pp. 57-8, 2010.
[108] D. Talbot, “Security in the ether,” Technology Review, vol. 113, no. 1, pp. 36-42, 2010.
[109] C. Teixeira, R. Azevedo, J. S. Pinto et al., "User Provided Cloud Computing," Proceedings 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGrid). pp. 727-32.
[110] P. J. Walsh, “The brightening future of cloud security,” Network Security, vol. 2009, no. 10, pp. 7-10, 2009.
[111] T. Spring, “Have data stored online? Protect it!,” PC World (San Francisco, CA), vol. 27, no. 8, pp. 12-13, 2009.
[112] D. Abraham, “Why 2FA in the cloud?,” Network Security, vol. 2009, no. 9, pp. 4-5, 2009.
[113] R. Chow, P. Golle, M. Jakobsson et al., "Controlling data in the cloud: Outsourcing computation without outsourcing control." pp. 85-90.
[114] CSA, "Top Threats to Cloud Computing V1.0," http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, [April 10, 2010, 2010].

[115] L. Hongwei, D. Yuanshun, T. Ling et al., "Identity-based Authentication for Cloud Computing," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 157-66.
[116] L. Yang, and A. Cemerlic, "Integrating dirichlet reputation into usage control."
[117] Y. Shucheng, W. Cong, R. Kui et al., "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," IEEE INFOCOM 2010 - IEEE Conference on Computer Communications. pp. 9 pp.-9 pp.
[118] D. J. Abadi, "Data Management in the Cloud: Limitations and Opportunities," 2009.
[119] K. Hwang, S. Kulkarni, and Y. Hu, "Cloud security with virtualized defense and reputation-based trust management." pp. 717-722.
[120] V. D. Cunsolo, S. Distefano, A. Puliafito et al., "Cloud@Home: Bridging the gap between volunteer and cloud computing," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 423-432.
[121] G. Briscoe, and A. Marinos, "Digital ecosystems in the clouds: Towards community cloud computing," 2009 3rd IEEE International Conference on Digital Ecosystems and Technologies, DEST '09. pp. 103-108.
[122] M. L. Yiu, G. Ghinita, C. S. Jensen et al., "Enabling search services on outsourced private spatial data," VLDB Journal, vol. 19, no. 3, pp. 363-384, 2010.
[123] G. Zhao, C. Rong, M. G. Jaatun et al., "Reference deployment models for eliminating user concerns on cloud security," Journal of Supercomputing, pp. 1-16, 2010.
[124] W. Wang, Z. Li, R. Owens et al., "Secure and efficient access to outsourced data." pp. 55-65.
[125] J. Sedayao, S. Su, M. Xiaohao et al., "A Simple Technique for Securing Data at Rest Stored in a Computing Cloud," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 553-8.
[126] A. Marinos, and G. Briscoe, "Community Cloud Computing," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 472-84.
[127] Z. Fengzhe, H. Yijian, W. Huihong et al., "PALM: security preserving VM live migration for systems with VMM-enforced protection," 2008 Third Asia-Pacific Trusted Infrastructure Technologies Conference. pp. 9-18.
[128] K. R. Joshi, G. Bunker, F. Jahanian et al., "Dependability in the cloud: Challenges and opportunities," Proceedings of the International Conference on Dependable Systems and Networks. pp. 103-104.
[129] C. Everett, "Cloud computing - a question of trust," Computer Fraud & Security, vol. 2009, no. 6, pp. 5-7, 2009.
[130] L. M. Kaufman, "Data security in the world of cloud computing," IEEE Security & Privacy, vol. 7, no. 4, pp. 61-4, 2009.
[131] W. Cong, W. Qian, R. Kui et al., "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," IEEE INFOCOM 2010 - IEEE Conference on Computer Communications. pp. 9 pp.-9 pp.
[132] R. Buyya, "Market-oriented cloud computing: vision, hype, and reality of delivering computing as the 5th utility," Proceedings of the 2009 Fourth ChinaGrid Annual Conference. ChinaGrid 2009. pp. 4 pp.-4 pp.
[133] R. Buyya, Y. Chee Shin, S. Venugopal et al., "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616, 2009.
[134] C. A. Dekkers, and P. A. McQuaid, "The dangers of using software metrics to (Mis)manage," IT Professional, vol. 4, no. 2, pp. 24-30, 2002.
[135] C. Martin, and M. Refai, "A policy-based metrics framework for information security performance measurement," 2nd IEEE/IFIP International Workshop on Business - Driven IT Management, BDIM' 07. pp. 94-5.
[136] C. Martin, and M. Refai, Service-oriented approach to visualize IT security performance metrics, 2007.

[137] A. Schwarz, B. Jayatilaka, R. Hirschheim et al., “A conjoint approach to understanding IT application services outsourcing,” Journal of the Association of Information Systems, vol. 10, no. 10, pp. 748-781, 2009.
[138] L. Martignoni, R. Paleari, and D. Bruschi, "A Framework for Behavior-Based Malware Analysis in the Cloud," Information Systems Security. Proceedings 5th International Conference, ICISS 2009. pp. 178-92.
[139] D. Remenyi, “A job for jack the cloud-slayer?,” IMIS Journal, vol. 18, no. 6, pp. 17-20, 2008.
[140] W. Du, G. Cui, and W. Liu, "A risk-aware reputation mechanism for resource sharing on grids," Proceedings - IEEE 9th International Conference on Computer and Information Technology, CIT 2009. pp. 223-227.
[141] M. Pastaki Rad, A. Sajedi Badashian, G. Meydanipour et al., "A survey of cloud platforms and their future," 2009, pp. 788-796.
[142] T. Biro, “A window to the world?,” Network Security, vol. 2009, no. 2, pp. 11-13, 2009.
[143] I. Keidar, “ACM SIGACT news distributed computing column 34 distributed computing in the clouds,” SIGACT News, vol. 40, no. 2, pp. 67-80, 2009.
[144] H. Kou, “Adaptive security model for communications on distributed environment using cloud models,” Jisuanji Gongcheng/Computer Engineering, vol. 32, no. 10, pp. 147-148+206-147-148+206, 2006.
[145] S. Hawkins, D. C. Yen, and D. C. Chou, “Awareness and challenges of Internet security,” Information Management and Computer Security, vol. 8, no. 3, pp. 131-143, 2000.
[146] W. Nauwelaerts, and P. Le Bousse, “Cloud busting: why cloud computing requires a new approach to data privacy,” Database and Network Journal, vol. 39, no. 6, pp. 17-19, 2009.
[147] I. Foster, Y. Zhao, I. Raicu et al., "Cloud Computing and Grid Computing 360-degree compared."
[148] J. Viega, “Cloud computing and the common man,” Computer, vol. 42, no. 8, pp. 106-8, 2009.
[149] H. G. Miller, and J. Veiga, “Cloud computing: Will commodity services benefit users long term?,” IT Professional, vol. 11, no. 6, pp. 57-59, 2009.
[150] D. McPherson, “Cybercrime - A game of cat and mouse in 2009,” Network Security, vol. 2010, no. 2, pp. 15-18, 2010.
[151] T. Takebayashi, H. Tsuda, T. Hasebe et al., “Data loss prevention technologies,” Fujitsu Scientific and Technical Journal, vol. 46, no. 1, pp. 47-55, 2010.
[152] S. Creese, P. Hopkins, S. Pearson et al., "Data protection-aware design for cloud services," 2009, pp. 119-130.
[153] O. Batarfi, and L. Marshall, "Defining criteria for rating an entity's trustworthiness based on its certificate policy." pp. 996-1003.
[154] K. Beaty, A. Kochut, and H. Shaikh, "Desktop to cloud transformation planning," 2009 IEEE International Symposium on Parallel Distributed Processing (IPDPS). pp. 8 pp.-8 pp.
[155] P. Murray, "Enterprise grade cloud computing." p. 1.
[156] N. Patel, and B. Marshall, "Examining the implications and challenges in cloud computing environments : An exploratory study."
[157] J. Schönwälder, M. Fouquet, G. D. Rodosek et al., “Future internet = content + services + management [Topics in Network and Service Management],” IEEE Communications Magazine, vol. 47, no. 7, pp. 27-33, 2009.
[158] Y. Arai, “Geographies of information society and cyberspace: A research perspective,” Japanese Journal of Human Geography, vol. 57, no. 1, pp. 47-67, 2005.
[159] A. C. Johnston, M. B. Schmidt, K. P. Arnett et al., “Getting to the root of the problem,” Journal of Internet Commerce, vol. 6, no. 1, pp. 1-12, 2007.
[160] T. Ristenpart, E. Tromer, H. Shacham et al., "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds." pp. 199-212.

[161] C. D. Cera, I. Braude, K. Taeseong et al., “Hierarchical role-based viewing for multilevel information security in collaborative CAD,” Transactions of the ASME. Journal of Computing and Information Science in Engineering, vol. 6, no. 1, pp. 2-10, 2006.
[162] “How to plug into the cloud [IT management],” InformationWEEK, no. 1214, pp. 20-2, 2008.
[163] “Implementing a secure virtual private network,” Elektron, vol. 20, no. 9, pp. 38-41, 2003.
[164] A. R. Choudhary, "In-depth analysis of IPv6 security posture."
[165] T. W. Wlodarczyk, C. Rong, and K. A. H. Thorsen, "Industrial cloud: Toward inter-enterprise integration," 2009, pp. 460-471.
[166] W. T. Tsai, Z. Jin, and X. Bai, "Internetware computing: Issues and perspective."
[167] R. C. Armstrong, and J. R. Mayo, "Leveraging complexity in software for cybersecurity."
[168] H. Zhao, M. Xu, N. Zheng et al., "Malicious executables classification based on behavioral factor analysis," IC4E 2010 - 2010 International Conference on e-Education, e-Business, e-Management and e-Learning. pp. 502-506.
[169] S. M. Tabish, M. Z. Shafiq, and M. Farooq, "Malware detection using statistical analysis of byte-level file content." pp. 23-31.
[170] R. Ford, and W. H. Allen, “Malware shall greatly increase,” IEEE Security and Privacy, vol. 7, no. 6, pp. 69-71, 2009.
[171] A. D. Schmidt, F. Peters, F. Lamour et al., “Monitoring smartphones for anomaly detection,” Mobile Networks and Applications, vol. 14, no. 1, pp. 92-106, 2009.
[172] R. Schwarzkopf, M. Schmidt, N. Fallenbeck et al., "Multi-layered virtual machines for security updates in grid environments," Conference Proceedings of the EUROMICRO. pp. 563-570.
[173] W. Goucher, “Out of office - and into trouble,” Computer Fraud and Security, vol. 2009, no. 8, pp. 16-18, 2009.
[174] S. D. Wolthusen, "Overcast: Forensic discovery in cloud environments," IMF 2009 - 5th International Conference on IT Security Incident Management and IT Forensics - Conference Proceedings. pp. 3-9.
[175] F. Zhang, Y. Huang, H. Wang et al., "PALM: Security preserving VM live migration for systems with VMM-enforced protection." pp. 9-18.
[176] M. A. Rajab, F. Monrose, A. Terzis et al., "Peeking through the cloud: DNS-based estimation and its applications," 2008, pp. 21-38.
[177] P. Goyal, and R. Mikkilineni, "Policy-based event-driven services-oriented architecture for cloud services operation management," CLOUD 2009 - 2009 IEEE International Conference on Cloud Computing. pp. 135-138.
[178] H. Xin, H. Yin, H. Yifan et al., "Privacy of Value-Added Context-Aware Service Cloud," Cloud Computing. Proceedings First International Conference, CloudCom 2009. pp. 547-52.
[179] A. Scolnik, “Protections for electronic communications: The stored communications act and the Fourth Amendment,” Fordham Law Review, vol. 78, no. 1, pp. 349-397, 2009.
[180] H. M. Kienle, and H. A. MÃ¼ller, "Research challenges in management and compliance of policies on the web." pp. 83-92.
[181] M. Yang, L. Wang, and Y. Lei, "Research on evaluation of trust model." pp. 345-349.
[182] J. Hale, and P. Brusil, “Secur(e/ity) management: A continuing uphill climb,” Journal of Network and Systems Management, vol. 15, no. 4, pp. 525-553, 2007.
[183] W. K. Wong, D. W. Cheung, B. Kao et al., "Secure kNN computation on encrypted databases." pp. 139-152.
[184] M. Schmidt, N. Fallenbeck, M. Smith et al., "Secure service-oriented grid computing with public virtual worker nodes." pp. 555-562.

[185] K. Sloan, “Security in a virtualised world,” Network Security, vol. 2009, no. 8, pp. 15-18, 2009.
[186] A. Ely, “Serious about security,” InformationWEEK, no. 1214, pp. 24-6, 2008.
[187] M. Sharmin, S. I. Ahamed, S. Ahmed et al., "SSRD+: A privacy-aware trust and security model for resource discovery in pervasive computing environment." pp. 67-70.
[188] E. P. F. d. L. Lausanne, "Stabilization Safety, and Security of Distributed Systems. Proceedings 11th International Symposium, SSS 2009." pp. xviii+801-xviii+801.
[189] D. G. Messerschmitt, "The consumer juggernaut: Web-based and mobile applications as innovation pioneer," 2009, pp. 1-7.
[190] “The devolution of security,” Information Age, pp. 23-5, 2009.
[191] A. S. Van Zyl, “The impact of Social Networking 2.0 on organisations,” Electronic Library, vol. 27, no. 6, pp. 906-918, 2009.
[192] W. Pieters, and A. van Cleeff, “The precautionary principle in a world of digital dependencies,” Computer, vol. 42, no. 6, pp. 50-56, 2009.
[193] “The state of e-mail security [the rise of cloud computing],” InformationWEEK, no. 1191, pp. 14-15, 2008.
[194] M. Dacier, V. H. Pham, and O. Thonnard, "The WOMBAT attack attribution method: Some results," 2009, pp. 19-37.
[195] J. Niu, Z. Chen, and G. Zhang, "Towards a subjective trust model with uncertainty for open network." pp. 102-109.
[196] V. M. García-Barrios, "User-centric privacy framework: Integrating legal, technological and human aspects into user-adapting systems." pp. 176-181.
[197] S. P. Subasingha, J. Zhang, K. Premaratne et al., "Using Association rules for classification from databases having class label ambiguities: A belief theoretic method," 2008, pp. 539-562.
[198] N. Gruschka, and L. L. Iacono, "Vulnerable cloud: SOAP message security validation revisited," 2009 IEEE International Conference on Web Services, ICWS 2009. pp. 625-631.
[199] W. Yan, and N. Ansari, "Why anti-virus products slow down your machine?," Proceedings - International Conference on Computer Communications and Networks, ICCCN.

APPENDIX A

LIST OF THREATS AND SECURITY ATTRIBUTES APPLICABLE IN CLOUD COMPUTING

The main outcome of phase 1 of this study is to identify threats and security attributes applicable in cloud computing. The threats and security attributes are listed as follows:

S/N	Threats	Threat Description	Source	Security Attribute Affected
1	Unclear ownership and responsibility of data protection	Lack of clear ownership and defined responsibilities for data protection may result in failure of meeting regulatory and legal obligations	[60] [61] [62]	Accountability
2	Identity theft	Identity theft in the cloud may lead to compromise of confidentiality and integrity of the data	[63] [64] [65] [66]	Integrity/Confidentiality (Authorization/ Authentication)
3	Unauthorized modification	Unauthorized modification of virtual images due to lack of adequate access controls	[67] [60]	Confidentiality, Integrity, Availability
4	Data theft	Data in the cloud machine is not be encrypted which results in breach of confidentiality	[61] [68, 69] [70, 71] [72]	Confidentiality
5	Malware attacks	Cloud clients may be attacked by malware injected in the cloud or in the network connection between cloud customer and cloud provider. Malware includes rootkit attack, Trojan horses, Cross Site-Scripting (XSS) attacks and viruses.	[61, 73] [74, 75] [65, 76] [77, 78] [79-81] [82, 83] [61]	Confidentiality, Integrity, Availability
6	Denial of service/Distributed Denial of Service (DOS/DDOS)	As a web based service, cloud is vulnerable to DOS attack leading to unavailability of cloud computing services	[61] [84] [85] [86, 87] [88] [50, 66] [6]	Availability
7	Lack of data segregation	In multi-tenancy cloud environment, there is a risk of one customer accessing or compromising data of other customers	[89] [90] [84] [91] [92, 93] [94]	Confidentiality, Integrity, Availability
8	Unauthorized access	Rogue users and service provider's staff may access cloud customers data due to extension of organization boundaries in the cloud	[90] [95] [96] [51] [97] [98] [99, 100] [101]	Integrity, Availability, Confidentiality
9	Data loss	Risks of losing data due to sharing in the cloud	[102] [103] [104]	Availability, Confidentiality
10	Data inconsistency	Risks of data inconsistency due to interfacing with internal systems that are not in the cloud. Further, data inconsistency may be caused by dynamic update (inserting, deletion, modification) from multiple customers.	[102] [105] [106]	Integrity
11	Eavesdropping	Data interception as the data might be transmitted in clear form	[90] [86] [107] [108] [109]	Confidentiality
12	Loss of business	Risk of cloud provider going out of business	[110] [111]	Availability, Accountability
13	Inadequate	Compromise of data security due to	[112] [113]	Confidentiality, Integrity,

S/N	Threats	Threat Description	Source	Security Attribute Affected
	authentication and authorization	inadequate authentication and authorization protection mechanism since cloud customers may not be able to enforce required controls.	[114] [63, 115] [116] [100] [117]	Availability
14	Insecure data storage	The risk of data being stored at an untrusted cloud provider resulting into compromise of privacy and data confidentiality.	[118] [91] [48] [119] [120] [121] [87] [122, 123] [124] [6] [125] [126]	Confidentiality
15	Cloud provider espionage	The worry of theft of company proprietary information by cloud provider	[113] [114] [66, 127]	Confidentiality
16	Service disruption	Disruption of business operations due to break down, unavailability of cloud services, or insufficient resource capacity provided by cloud provider	[84] [103] [128] [87] [51] [123] [6] [126]	Availability
17	Phishing attack	Phishing/social engineering attacks to cloud provider	[113] [114]	Confidentiality
18	Audit difficulty	Audit difficulty of third party cloud provider as the data maybe distributed across several geographical locations	[113] [114] [129] [130] [131]	Accountability
19	Insecure Interfaces and APIs	Insecure API including weak authentication and access control may compromise of cloud customers information	[114]	Confidentiality, Integrity
20	Regulatory and legal issues	Difficult to enforce customers' IT legal and regulatory issues as the data is stored outside the organizations	[132] [6, 133] [61]	Accountability
21	Difficult bugs detection	Cloud providers face difficulty in detecting bugs in cloud environment as it has huge database as well as high number of services and customers	[50]	Accountability
22	Difficult intruder (malicious user) detection	Difficult to detect intruder as the cloud is accessed by multiple users from many different customers using simple devices.	[50]	Accountability

APPENDIX B

LIST OF IDENTFIED FRAMEWORKS FOR DEVELOPING SECURITY METRICS AND THEIR APPROPRIATE SCORES

In this section, the identified frameworks for developing security metrics and their appropriate scores are presented here. These are the end outcome of phase 2 of this study.

S/N	Framework Name	Framework Description (Feature/step)	Source	Individual Framework Score				Accumulated score	Remarks
				Simplicity	Acceptability	Universality	Intended Audience		
1	EBPP	Metrics for Electronic bill presentment and payment (EBPP) system by identifying threats using STRIDE (Spoofing identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) model. The threats along with components of the architecture are tied together in a framework model to measure the security levels in place. Step-by-step procedure to derive an overall security rating for EBPP system i) Security and criticality index assessment of individual components ii) Determination of ratings for the STRIDE threats iii) Mapping of the transaction flow states for the three state–transition diagrams across components. iv) Assessment of STRIDE threats faced by various states of the state diagrams.	[39]	3	2	2	1	8	Developed for a specific system the EBPP and has not been validated

S/N	Framework Name	Framework Description (Feature/step)	Source	Individual Framework Score				Accumulated score	Remarks
				Simplicity	Acceptability	Universality	Intended Audience		
		v) Computation of the vulnerabilities and normalized threat sets for states of the state diagrams. vi) Consolidation of state vulnerabilities at state diagram level. vii) Derivation of the final security score							
2	ROCONA	The authors proposed comprehensive security metric framework called Risk based proactive security cOnfiguration manager (ROCONA). Security metric for measuring proactive security configuration in a network is by identifying, formulating, and validating several important risk factors that greatly affect network security including existing and future vulnerabilities. The stages of the framework are: i) Traffic risk analysis ii) Service risk analysis iii) Policy risk analysis iv) Threat probability calculation v) Threat impact vi) Network risk measure vii) Security score and recommendations	[53]	2	3	2	2	9	Developed for a specific purpose of measuring security configuration in a network. No evidence of validation in academia or industry.
3	Goal Question Metric	Measurement is defined in top-down fashion which focusing and basing on goals and models. Basic stages Goal, Metric, Question Six sub-steps of GQM process: i) Develop business goals ii) Generate questions	[28] [134]	4	4	5	5	18	It is a well researched generic framework that follows a goal based approach and which has been in use for long time. The framework is

S/N	Framework Name	Framework Description (Feature/step)	Source	Individual Framework Score				Accumulated score	Remarks
				Simplicity	Acceptability	Universality	Intended Audience		
		iii) Specify the measures iv) Develop mechanisms v) Collect, validate and analyze the data in real time vi) Analyze the data in a post-mortem							considered simple to use and suitable to produce metrics for the intended audiences.
4	Framework for policy based metrics	The authors used approach specified in NIST 800-53 and NIST SP800-80 to measure and monitor overall IT security performance in an organization and propose framework for policy based metrics approach i) Security Policies and Procedures Model ii) Security Goals and Targets Achievement iii) Security Measurement Processes iv) Metrics development and analysis v) Metrics and Measurement Model vi) Reporting analysis and agent vii) Report and recommendation module	[135] [136]	4	2	2	3	11	The framework rely on organizations policies. In addition, the framework is based on superseded US NIST guidelines.
5	Security Metric Identification Framework	The framework provides a systematic method to identify or develop security metric suite for software. The framework has not been validated in the industry. It has ten stages namely: i) Specify Security Metrics Requirements ii) Identify Vulnerability iii) Identify Software Characteristics iv) Analyze OO Models v) Analyze Security Metrics vi) Categorize Security Metrics vii) Specify Security Metric Measures viii) Design Metric Development Process	[54]	2	1	1	2	6	Is a newly proposed framework and has not been validated. Moreover, the framework is considered complicated for practical use.

S/N	Framework Name	Framework Description (Feature/step)	Source	Individual Framework Score				Accumulated score	Remarks
				Simplicity	Acceptability	Universality	Intended Audience		
		ix) Design Security Metric x) Finalize Metric Suite							
6	NIST SP800-55	This framework contains two stages: i) Information Security Measures Development Process a. Stakeholders interest identification b. Goals and objective identification c. Information security policies, guidelines, and procedures review d. Information security program implementation review e. Measures development and selection f. Measures development template g. Feedback within the measures development process ii) Information Security Measurement Program Implementation process a. Prepare for data collection b. Collect data and analyze result c. Identify corrective actions d. Develop business case and obtain resources e. Apply corrective actions	[34]	5	3	5	4	17	It is a well researched generic framework that follows a goal based approach. The framework is considered simple to use and suitable to produce metrics for the intended audiences. Intended for official use in US government organizations hence suffers global acceptance.
7	SANS security metrics guideline	The guideline has seven stages: i) Define the metrics program goal(s) and objectives ii) Decide which metrics to generate iii) Develop strategies for generating the metrics iv) Establish benchmarks and targets	[40]	4	4	3	4	15	It is a generic framework that follows a goal based approach. The framework is considered simple to

S/N	Framework Name	Framework Description (Feature/step)	Source	Individual Framework Score				Accumulated score	Remarks
				Simplicity	Acceptability	Universality	Intended Audience		
		v) Determine how the metrics will be reported vi) Create an action plan and act on it, and vii) Establish a formal program review/refinement cycle							use and suitable to produce metrics for the intended audiences. The complete documentation could not be obtained
8	Security Performance Framework (SPF)	Proposed Security Performance Framework (SPF) to measure and monitor overall IT security performance in an organization using NIST SP800-80 approaches. The SPF follows two approaches: i) Control-specific approach selects individual controls as the basis for a metric that best represents the entire family as determined by the organizational environment. ii) The cross-cutting approach focuses on metrics that gauge security performance based on more than one individual control or control families. Multiple controls or control families are used in the development, collection, and analysis of the metric.	[135]	4	2	2	3	11	The framework relies on organizations policies. In addition, the framework is based on superseded US NIST guidelines.

APPENDIX C1

COBIT IT PROCESSES THAT MET OBJECT SELECTION CRITERIA

S/N	Process Name	Abbreviation
1.	Assess and Manage IT Risks	PO9
2.	Enable Operation and Use	AI4
3.	Manage Changes	AI6
4.	Install and Accredit Solutions and Changes	AI7
5.	Manage Performance and Capacity	DS3
6.	Ensure Continuous Service	DS4
7.	Ensure Systems Security	DS5
8.	Manage Service Desk and Incidents	DS8
9.	Manage the Configuration	DS9
10.	Manage Problems	DS10
11.	Manage Data	DS11
12.	Manage Operations	DS13
13.	Monitor and Evaluate Internal Control	ME2
14.	Ensure Compliance With External Requirements	ME3

APPENDIX C2

IDENTIFICATION OF SECURITY OBJECTS

COBIT IT Process	Criteria		
	Related with Information Security	Relevant in the cloud	Tasks performed by Cloud Provider
Plan and Organize			
PO1 Define a Strategic IT Plan	NO	NO	NO
PO2 Define the Information Architecture	YES	YES	NO
PO3 Determine Technological Direction	YES	YES	NO
PO4 Define the IT Processes, Organisation and Relationships	YES	YES	NO
PO5 Manage the IT Investment	YES	YES	NO
PO6 Communicate Management Aims and Direction	YES	YES	NO
PO7 Manage IT Human Resources	YES	YES	NO
PO8 Manage Quality	YES	YES	NO
PO9 Assess and Manage IT Risks	YES	YES	YES
PO10 Manage Projects	NO	NO	NO
Acquire and Implement			
AI1 Identify Automated Solutions	YES	YES	NO
AI2 Acquire and Maintain Application Software	YES	YES	NO
AI3 Acquire and Maintain Technology Infrastructure	YES	YES	NO
AI4 Enable Operation and Use	YES	YES	YES
AI5 Procure IT Resources	YES	YES	NO
AI6 Manage Changes	YES	YES	YES
AI7 Install and Accredit Solutions and Changes	YES	YES	YES
Deliver and Support			
DS1 Define and Manage Service Levels	YES	YES	NO
DS2 Manage Third-party Services	YES	YES	NO
DS3 Manage Performance and Capacity	YES	YES	YES
DS4 Ensure Continuous Service	YES	YES	YES
DS5 Ensure Systems Security	YES	YES	YES
DS6 Identify and Allocate Costs	YES	NO	NO
DS7 Educate and Train Users	YES	YES	NO
DS8 Manage Service Desk and Incidents	YES	YES	YES
DS9 Manage the Configuration	YES	YES	YES
DS10 Manage Problems	YES	YES	YES
DS11 Manage Data	YES	YES	YES

COBIT IT Process	Criteria		
	Related with Information Security	**Relevant in the cloud**	**Tasks performed by Cloud Provider**
DS12 Manage the Physical Environment	YES	YES	NO
DS13 Manage Operations	YES	YES	YES
Monitor and Evaluate			
ME1 Monitor and Evaluate IT Performance	YES	YES	NO
ME2 Monitor and Evaluate Internal Control	YES	YES	YES
ME3 Ensure Compliance With External Requirements	YES	YES	YES
ME4 Provide IT Governance	YES	NO	NO

APPENDIX D

LIST OF IDENTIFIED SLA BASED INFORMATION SECURITY METRICS IN CLOUD COMPUTING

In this section, SLA based information security metrics in cloud computing as the main outcome of this study are presented here.

Goal 1	Purpose	Evaluate (cloud computing)
	Issue	Adequacy of
	Object (process)	Configuration management
	Viewpoint	Senior managers
Question	Q1	What are the impacts of improper configurations to the business caused by cloud provider?
Metrics	M1	Number of security incidents or noncompliance issues caused by improper configuration [10]
	M2	Number of occurrence of financial loss due to license violations[10]
Question	Q2	How adequately is the cloud provider managing IT asset configurations?
Metrics	M1	Number of deviations identified between the configuration repository and actual asset configurations
Goal 2	Purpose	Evaluate (cloud computing)
	Issue	Effectiveness of
	Object (process)	Change management
	Viewpoint	Senior managers
Question	Q1	What is an average time to complete a change request?
Metrics	M1	Mean Time to Complete Changes [11] $MTCC = \frac{CompletionDate - SubmissionDate}{Count(completedChanges)}$
Question	Q2	How does inadequate change management procedure negatively impact business operations?
Metrics	M1	Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment [10]
	M2	Amount of application rework caused by inadequate change specifications [10]
	M3	% of unsuccessful changes caused by inadequate change specifications [10]
Goal 3	Purpose	Evaluate (cloud computing)
	Issue	Timeliness or Effectiveness of
	Object (process)	Problems and incident management
	Viewpoint	Senior managers
Question	Q1	What is the average time taken by the cloud provider to resolve a security incident
Metrics	M1	Average duration of resolving security incidents by severity [10]
	M2	% of security incidents resolved within an acceptable timeframe [10]
Question	Q2	To what extent is the business operations affected by security incidents

Metrics	M1	Number of security incidents with potential impact to the business operations [10]
	M2	Number of business disruptions due to IT service disruption [10]
	M3	Hours of unplanned downtime caused by operational incidents [10]
	M4	Number of recurring problems with an impact on the business [10]
Question	Q3	What is the time between occurrence of a security incident and its discovery?
Metrics	M1	Mean-Time-To-Incident-Discovery [10] $MTDF = \frac{\sum (\text{Date\_of\_Discovery - Date\_of\_Occurrence})}{\text{Count(Incidents)}}$ [11]
Question	Q4	How much time is taken to resume business operations after occurrence of a security incident?
Metrics	M1	Mean Time To Incident Recovery (MTTIR) [10] $MTTIR = \frac{\sum (\text{Date\_of\_Recovery - Date\_of\_Occurrence})}{\text{Count(Incidents)}}$
Goal 4	Purpose	Analyze (cloud computing)
	Issue	Effectiveness of
	Object (process)	Risk management
	Viewpoint	Senior Managers
Question	Q1	How effective is the cloud client risk management?
Metrics	M1	% of identified critical IT events that have been assessed [10]
	M2	Number of significant incidents caused by risks that were not identified by the risk assessment process [10]
	M3	% of identified critical IT risks that has been addressed [10]
	M4	% of critical IT components (applications and network infrastructure) covered by risk assessment [10]
Goal 5	Purpose	Analyze (cloud computing)
	Issue	Effectiveness in handling
	Object (process)	Compliance issues
	Viewpoint	Senior managers
Question	Q1	Is the cloud provider adhering to Service Level Agreement?
Metrics	M1	Number of formal disputes with cloud provider [10]
	M2	Number of regulatory or legal noncompliance events caused by cloud provider [10]
	M3	Number of user complaints due to contracted services [10]
Question	Q2	How is the cloud client affected due to IT non-compliance?
Metrics	M1	Cost of IT non-compliance, including settlements and fines [10]
	M2	Number of non-compliance issues causing public comment or embarrassment [10]
	M3	% of security breaches (incidents) caused by non-compliance issues [10]
Question	Q3	Are there clearly defined and assigned security responsibilities between the cloud provider and the client?
Metrics	M1	Number of escalations or unresolved security issues due to lack of, or insufficient assigned responsibilities. [10]
Question	Q4	Do applications and platforms comply with standards agreed between cloud client and provider?
Metrics	M1	Percent of applications not complying with the information architecture and technology standards [10]

	M2	Percent of platforms not complying with the defined IT architecture and technology standards [10]
Goal 6	Purpose	Analyze (cloud computing)
	Issue	Adequacy of
	Object (process)	Operations management
	Viewpoint	Senior managers
Question	Q1	How is the cloud client affected by inadequate operations management of the cloud provider?
Metrics	M1	Number of service levels impacted by operational incidents emanating from the provider [10]
	M2	Hours of unplanned downtime caused by operational incidents [10]
	M3	Percent of scheduled work and requests not completed on time by the cloud provider [10]
Goal 7	Purpose	Analyze (cloud computing)
	Issue	Effectiveness of
	Object (process)	Performance and capacity management
	Viewpoint	Senior managers
Question	Q1	Does the cloud provider sufficiently manage performance and capacity of IT systems?
Metrics	M1	% of response time SLA not met [10]
	M2	Number of hours lost per business operations per month due to insufficient capacity planning [10]
	M3	Transaction failure rate due to poor performance of IT systems [10]
Goal 8	Purpose	Analyze (cloud computing)
	Issue	Effectiveness of
	Object (process)	Continuity of IT services
	Viewpoint	Senior managers
Question	Q1	To what extent do critical systems meet agreed continuity of IT services?
Metrics	M1	% of tests of critical systems that achieve recovery objectives [10]
	M2	Number of hours of down time per critical systems [10]
Goal 9	Purpose	Analyze (cloud computing)
	Issue	Effectiveness of
	Object (process)	IT Security management
	Viewpoint	Senior managers
Question	Q1	How effective is the cloud provider in detecting and resolving security vulnerabilities?
Metrics	M1	% of systems where security requirements are not met [10]
	M2	Number of violations in segregation of duties [10]
Question	Q1	How timely does the client provider discover and apply security patches and fixes?
Metrics	M1	Time lag between release of security patches and when the patches are installed in the affected systems [10] Mean Time to Patch (MTTP) $\text{MTTP} = \frac{\sum(\text{DateOfInstallation} - \text{DateOfAvailability})}{\text{Count}(\text{CompletedPatches})}$

Goal 10	Purpose	Analyze (cloud computing)
	Issue	Effectiveness of
	Object (process)	Application software management
	Viewpoint	Senior managers
Question	Q1	How do application software problems and defects affect business operations?
Metrics	M1	Number of production problems per application causing visible downtime [10]
	M2	Number of reported defects per application per month [10]

APPENDIX E

PILOT DATA USED TO COMPUTE COHEN'S KAPPA FOR SLR1

S/N	Title	Researcher 1	Researcher 2
1.	Young Australian's Privacy, Security and Trust in Internet Banking	Yes	No
2.	XPay Practical anonymous payments for Tor Routing and other networked services	No	No
3.	Wrap Scientific Applications as WSRF Grid Services using gRAVI	No	No
4.	Wireless communications using millimeter-wave beams carrying orbital angular momentum	No	No
5.	Wikipedia-Graph Based Key Concept Extraction Towards News Analysis	No	No
6.	Why anti-virus products	No	No
7.	Why 2FA in the cloud?	Yes	Yes
8.	Whats in store for 2010	Yes	Yes
9.	Weather Modification	No	No
10.	Vulnerable Cloud: SOAP Message Security Validation Revisited	Yes	Yes
11.	Visualizations of human activities in sensor-enabled ubiquitous environments	No	No
12.	Virtual clusters for grid, cloud, and high-performance computing	No	No
13.	Virtual business networks with cloud computing and virtual machines	Yes	Yes
14.	Using RESTful web-services and cloud computing to create next generation mobile applications	No	No
15.	Using LIDAR-based	Yes	No
16.	Using Computational	No	No
17.	User-level virtual network support for sky computing	Yes	Yes
18.	User Requirements for Cloud Computing Architecture	Yes	Yes
19.	User Provided Cloud Computing	Yes	No
20.	Use of Advanced Techniques to Model the Dispersion	No	No

APPENDIX F

PILOT DATA USED TO COMPUTE COHEN'S KAPPA FOR SLR2

S/N	Title	Researcher 1	Researcher 2
1.	Pareto-optimal situaton analysis for selection of security measures	No	No
2.	Privacy preserving data mining algorithms by data distortion	No	No
3.	Program partitioning using dynamic trust models	No	No
4.	Queueing analysis for OFDM subcarrier allocation in broadband wireless multiservice networks	No	No
5.	RePro	No	No
6.	Risk as dependability metrics for the evaluation of business solutions	Yes	Yes
7.	Risk management in the trustworthy software process	No	Yes
8.	Security engineering developments and directions	No	No
9.	Security interface between Metrica and Magerit development of secure information systems	Yes	Yes
10.	Software quality from a behavioral perspective	No	No
11.	Spaceport models assessment	Yes	Yes
12.	Specifying and measuring quality of service in distributed object systems	No	No
13.	Survey of psychophysiology measurements applied to human-robot interaction	No	No
14.	Synergistic verification and validation of systems and software engineering models	No	No
15.	The dangers of using software metrics to (Mis)manage	Yes	Yes
16.	Tow test results of an AquaPod fish cage	No	No
17.	Toward the use of automated static analysis alerts for early identification of vulnerability	No	No
18.	Unit testing non-functional concerns of component-based distributed systems	No	No
19.	Using importance flooding to identify interesting networks of criminal activity	No	No
20.	Water and economic development	No	No

APPENDIX G

LIST OF STUDIES RELEVANT FOR SLR1

S/N	Paper Title	Source	Year of Publication
1.	A conjoint approach to understanding IT application services outsourcing	[137]	2009
2.	A framework for behavior-based malware analysis in the cloud	[138]	2009
3.	A job for jack the cloud-slayer?	[139]	2008
4.	A privacy manager for cloud computing	[95]	2009
5.	A risk-aware reputation mechanism for resource sharing on grids	[140]	2009
6.	A survey of cloud platforms and their future,	[141]	2009
7.	A window to the world?	[142]	2009
8.	Accountability as a way forward for privacy protection in the cloud	[62]	2009
9.	ACM SIGACT news distributed computing column 34 distributed computing in the clouds	[143]	2009
10.	Adaptive security model for communications on distributed environment using cloud models'	[144]	2006
11.	APFA: Asynchronous parallel finite automaton for deep packet inspection in cloud computing	[49]	2009
12.	Awareness and challenges of Internet security	[145]	2000
13.	Bridging the missing link of cloud data storage security in AWS	[60]	2010
14.	Can a trusted environment provide security?	[93]	2010
15.	Cloud busting: why cloud computing requires a new approach to data privacy	[146]	2009
16.	Cloud Computing and Grid Computing 360-degree compared	[147]	2008
17.	Cloud computing and the common man	[148]	2009
18.	Cloud computing: Will commodity services benefit users long term?	[149]	2009

S/N	Paper Title	Source	Year of Publication
19.	Cloud security is not (just) virtualization security: A short paper	[76]	2009
20.	Cloud security issues	[3]	2009
21.	Controlling data in the cloud: Outsourcing computation without outsourcing control	[113]	2009
22.	Cybercrime - A game of cat and mouse in 2009	[150]	2010
23.	Danger in the clouds	[84]	2008
24.	Data loss prevention technologies	[151]	2010
25.	Data protection-aware design for cloud services	[152]	2009
26.	Defining criteria for rating an entity's trustworthiness based on its certificate policy	[153]	2006
27.	Desktop to cloud transformation planning	[154]	2009
28.	Enterprise grade cloud computing	[155]	2009
29.	Examining the implications and challenges in cloud computing environments : An exploratory study	[156]	2009
30.	Future internet = content + services + management [Topics in Network and Service Management]	[157]	2009
31.	Geographies of information society and cyberspace: A research perspective	[158]	2005
32.	Getting to the root of the problem	[159]	2007
33.	Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds	[160]	2009
34.	Hey, you, get off of that cloud?	[70]	2009
35.	Hierarchical role-based viewing for multilevel information security in collaborative CAD	[161]	2006
36.	How to plug into the cloud [IT management]	[162]	2008
37.	ID management among clouds	[63]	2009
38.	Implementing a secure virtual private network	[163]	2003
39.	In-depth analysis of IPv6 security posture	[164]	2009
40.	Industrial cloud: Toward inter-enterprise integration	[165]	2009
41.	Integrating dirichlet reputation into usage control	[116]	2009

S/N	Paper Title	Source	Year of Publication
42.	Internetware computing: Issues and perspective	[166]	2009
43.	Leveraging complexity in software for cybersecurity	[167]	2009
44.	Malicious executables classification based on behavioral factor analysis	[168]	2010
45.	Malware detection using statistical analysis of byte-level file content	[169]	2009
46.	Malware shall greatly increase	[170]	2009
47.	Managing security of virtual machine images in a cloud environment	[67]	2009
48.	Monitoring smartphones for anomaly detection	[171]	2009
49.	Multi-layered virtual machines for security updates in grid environments	[172]	2009
50.	On technical security issues in cloud computing	[61]	2009
51.	Out of office - and into trouble	[173]	2009
52.	Outlook: Cloudy with a chance of security challenges and improvements	[89]	2010
53.	Overcast: Forensic discovery in cloud environments	[174]	2009
54.	PALM: security preserving VM live migration for systems with VMM-enforced protection	[175]	2008
55.	Peeking through the cloud: DNS-based estimation and its applications	[176]	2008
56.	Policy-based event-driven services-oriented architecture for cloud services operation management	[177]	2009
57.	Privacy as a service: privacy-aware data storage and processing in cloud computing architectures	[98]	2009
58.	Privacy of value-added context-aware service cloud	[178]	2009
59.	Protections for electronic communications: The stored communications act and the Fourth Amendment	[179]	2009
60.	Research challenges in management and compliance of policies on the web	[180]	2008
61.	Research on evaluation of trust model	[181]	2008
62.	Secur(e/ity) management: A continuing uphill climb	[182]	2007
63.	Secure kNN computation on encrypted databases	[183]	2009

S/N	Paper Title	Source	Year of Publication
64.	Secure service-oriented grid computing with public virtual worker nodes	[184]	2009
65.	Security in a virtualised world	[185]	2009
66.	Security in the ether	[108]	2010
67.	Serious about security	[186]	2008
68.	SSRD+: A privacy-aware trust and security model for resource discovery in pervasive computing environment	[187]	2006
69.	Stabilization Safety, and Security of Distributed Systems	[188]	2009
70.	The brightening future of cloud security," Network Security	[110]	2009
71.	The consumer juggernaut: Web-based and mobile applications as innovation pioneer	[189]	2009
72.	The devolution of security	[190]	2009
73.	The impact of Social Networking 2.0 on organisations	[191]	2009
74.	The precautionary principle in a world of digital dependencies	[192]	2009
75.	The state of e-mail security [the rise of cloud computing]	[193]	2008
76.	The WOMBAT attack attribution method: Some results	[194]	2009
77.	Towards a subjective trust model with uncertainty for open network	[195]	2006
78.	User-centric privacy framework: Integrating legal, technological and human aspects into user-adapting systems	[196]	2009
79.	Using Association rules for classification from databases having class label ambiguities: A belief theoretic method,	[197]	2008
80.	Vulnerable cloud: SOAP message security validation revisited,	[198]	2009
81.	Why 2FA in the cloud	[112]	2009
82.	Why anti-virus products slow down your machine?	[199]	2009