Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.815 – 831

RESEARCH ARTICLE

A Semantic Ontology based Concept for Measuring Security Compliance of Cloud Service Providers

Mustafa Nouman Murad Al-Hassan

M.Sc., Computer Information Systems, Middle East University, Jordan

mustafa@orasnet.com

Abstract— Cloud computing is Internet-based computing, whereby shared resources, software and information, are provided with computers and devices on-demand. It also makes security problems more complicate and more important for Cloud Service Provider (CSP) and consumer than before. International standard organizations issue security-related standards and guidance which can be used in cloud environment such as ISO/IEC 27001. This research explores the possibility to measure security compliance for data breaches threat based semantic similarity measure between the documents of international standard compliments and CSP response against data breaches threat.

We developed a model for that purpose. Our model consists of three stages: (1) Extracting ontology concepts of CC threat (2) Extracting ontology concepts of CSP (3) Matching Process among the both ontology concepts. The matching process has done by using semantic similarity measure. Also during our study, we collected and studied many documents and reports that discussed data breaches threat. Then we classified it into group of (Control Area), identify the items that cover each control area. Also tested 5 CSPs to measure their security compliance by collection their data related to each control area; then convert it into text file in order extracting ontology concepts.

Keywords— Cloud Computing; Security Compliance; Data Breach, Ontology Concept; Semantic Similarity

I. INTRODUCTION

A. Cloud Computing

Cloud Computing (CC) is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, CC describes applications that are extended to be accessible through the internet and for this purpose large data centres and powerful servers are used to host the web applications and web services [4]. CC [1] provides the next generation of internet based, highly scalable distributed computing systems in which computational resources are Cloud Service Providers (CSPs) offer cloud platforms for their customers to use and create their web services, much like internet service providers (ISP) offer customers high speed broadband to access the internet. CSPs and ISPs both offer services. The cloud provides a layer of abstraction between the computing resources and the low level architecture involved. The customers do not own the actual physical infrastructure but merely pay a subscription fee and the CSP grants them access to the clouds resources and infrastructure. A key concept is that the customers can reduce expenditure on resources like software licenses, hardware and other services (e.g. email) as they can obtain all these things from one source, the CSP [12].

B. CC Security

CC is designed to be successful by reducing overhead and improving efficiency. With those improvements come the loss of control and possible security risk to the data [4] the leading U.S. market research firm Gartner released a report "Assessing the Security Risks of Cloud Computing" in June 2008. This report stated that cloud computing has great risk to data integrity, data recovery and privacy, etc. [18].

There are still many open and interesting issues regarding CC paradigm and standards are still evolving. But, it is a general opinion that security is indeed one of the most important issues [26]. In the recent IDC report over 74.6% in 2008 Fig. 1. and 87.5% in 2009 Fig. 2. of users think that security is a dominant issue for widespread use of CC services.

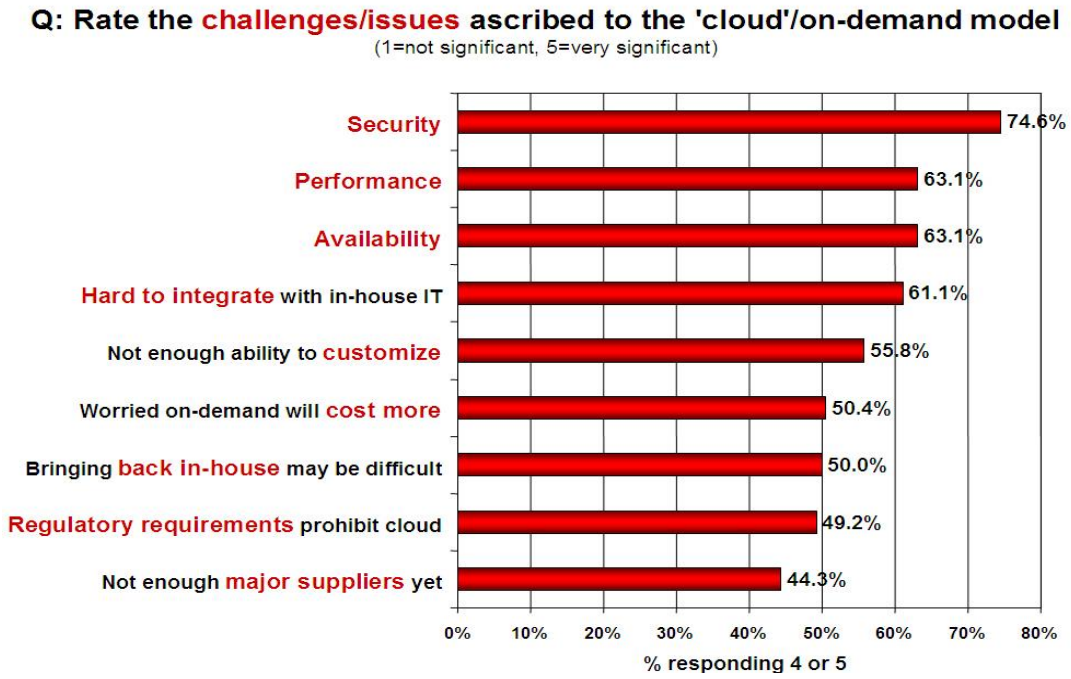

Fig. 1 Importance of Security for CC Environments 2008

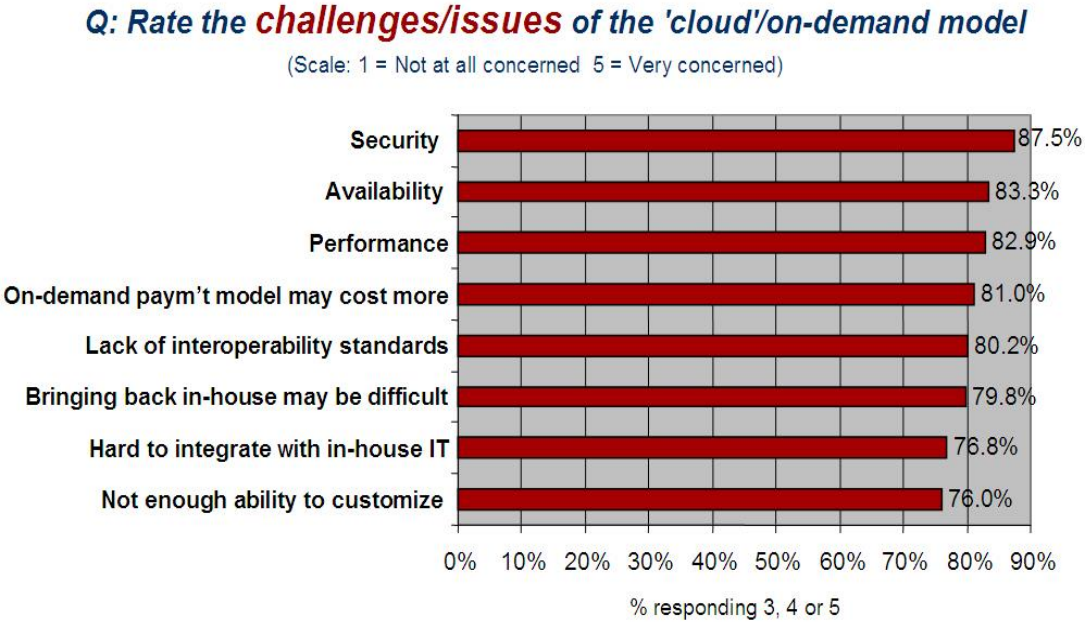

Fig. 2 Importance of Security for CC Environments - 2009

Like traditional computing environments, CC brings risks and security concerns to the organizations 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 (CSP) [20]. CSP has recognized the cloud security concern and are working hard to address it. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software [21].

In CC environment, overall security issues can be evaluated from the points of CSP and the consumer. While the CSP focus on the continuity of their services against configuration updates for performance and QoS, spam and virus threats and proper customer accountability, clients mainly look for the security of their data and the reliability of the provider [41].

Academics and security products manufacturers are actively studying CC data security [33]. However there still exist many problems with cloud computing today. A recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing [33]. Due to the above challenges and threats cloud customers therefore need to institute mechanisms to measure and improve the 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 metric [31].

C. Data Breaches Threat

A Data Breach is the intentional or unintentional release of secure information in an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak and also data spill [35]. In CC and according the Cloud Security Alliance (CSA) report "Top 10 threats in Cloud Computing"; the data breaches threat is ranking No.5 in 2010 [8] and No.1 in 2013 [9]; and it's in the high risk level Risk Matrix Fig. 3. and Fig. 4.

Fig. 3 Data Breaches Threat Top Ranking 2013

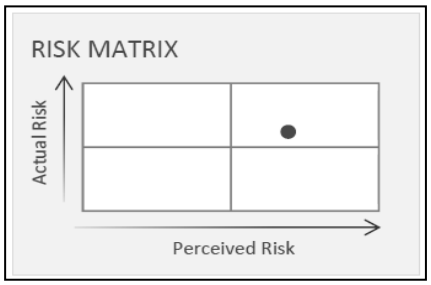

Fig. 4 Data Breaches Threat in very high in Risk Matrix

The data breaches in CC associated with the (11) parameters called Controls Area (CA) [9] as shown in Table 1. The full specifications of each CA for data breach threat:

TABLE I
THE CLASSIFICATION FOR DATA BREACHES THREAT

No.	Control Area (CA)	Control ID
1	Data Governance - **Retention Policy**	DG-04
2	Data Governance - **Secure Disposal**	DG-05
3	Data Governance - **Non-Production Data**	DG-06
4	Data Governance - **Information Leakage**	DG-07
5	Data Governance - **Risk Assessments**	DG-08
6	Information Security - **Encryption**	IS-18
7	Information Security - **Encryption Key Management**	IS-19
8	Security Architecture - **User ID Credentials**	SA-02
9	Security Architecture - **Data Security / Integrity**	SA-03
10	Security Architecture - **Production / Non-Production Environments**	SA-06
11	Security Architecture - **Remote User Multi-Factor Authentication**	SA-07

D. Security Compliance

Security compliance distinguishes it from security itself. While security refers to a mechanism that have to be used in order for a system to be in a safe state from prospective threats, security compliance refers to a state of compliance with a given set of security requirements. Therefore, while security it is used to protect a system from threats, security compliance has nothing to do with this protection. Rather, security compliance ensures that the security measures taken to protect the system are compliant with the necessary requirements [37]. Klaus Julisch from IBM Research has defined the security compliance as follows [19]:

"*Security compliance, in IT systems, is the state of conformance with externally imposed functional security requirements and of providing evidence (assurance) thereof.*"

These days security compliance generally indicates the compliance with industry accepted security standards such as NIST, ISO 270001/27002, HIPAA, PCI DSS, etc. While compliance helps drive security, it does not equal actual security.

The 2011 Data Breach Investigation Report [2] outlined the fact that non-compliance is one of the main reasons for data breaches in the Payment Card Industry (PCI). In this report, it was stated that 96% of the companies that suffered the breach have not achieved compliance with the PCI DSS. Only the remaining 4% of companies were still under attack despite having achieved the compliance with PCI DSS. This is a clear indication of how much difference can it make to have the security compliance.

E. Ontology and Semantic Similarity

Ontology; is an abstract description system for knowledge composition in a certain domain. By organizing concepts (terms) in a domain in a hierarchical way and describing relationships between terms using a small number of relational descriptors, an ontology supplies a standardized vocabulary for representing entities in the domain [17].

Semantic similarity is a concept whereby a set of documents or terms within term lists assign a metric based on the likeness of their meaning / semantic content. Various semantic similarity techniques are available which can be used for measuring the semantic similarity between text documents [27].

F. Problem Definition

The CC offers dynamically scalable resources provisioned as a service over the Internet. Each CSPs has own security requirements. We need to unify and measure the majority of cloud security compliance and requirements in order to the evaluate the level of the security of his cloud. This will lead to several problems to be identified as follows:

1. How can we classify the different parameters of CC threats?
2. How can we build a unified classification measure of the data breaches threat?
3. How to automate the measure (semantically) for the each CSP compliances to mitigate data breaches threats?
4. How to deploy semantic similarity measure to rank the CSP according CC threat.

II. **RELATED WORD**

In 2010, Reference [13] proposed a methodology for automatically generating ISO 27001-based IT-security metrics and showed how the security ontology can be used to generate concrete and organization-specific knowledge regarding existing control implementations. In the example of ISO 27001, author showed that the developed methodology supports organizations in evaluating (1) their compliance to information security standards, and (2) the effectiveness of existing control implementations. The authors took some concept from this research to create ontology for the controls of the data breaches threat on the CC base on major compliance international standards.

In 2010, Reference [24] presented the view on the importance and challenges of developing a security metrics framework for the Cloud, also taking into account ongoing research with organizations like the Cloud Security Alliance (CSA) and European projects like ABC4Trust, CoMiFin and INSPIRE. The authors also introduced the basic building blocks of a proposed security metrics framework for elements such as a CSP security assessment, taking into account the different service and deployment models of the Cloud.

In 2012, Reference [29] proposed a framework consists of eight domains which can be further divided into sub domains. All these domains should comply with various regulations and government policies like SOX, FISMA, HIPAA, COBIT, ISO/IEC 27001/2, etc. accordingly.

In 2012, Reference [34] discussed security issues of cloud computing, and proposed basic building blocks of information security metrics framework for cloud computing. The information security metrics framework has four major stages: 1) Metrics Preparation the IS metrics preparation phase involves information security metrics development team to develop useful information security metrics. 2) Threat Identification and Analysis The 2nd Phase of this proposed framework is about threat elicitation and analysis. In this phase, the threats are identified from information security metrics and different techniques like threat tree are applied to analyze the threat 3) Threat Processing After Analysis of threat, this phase is defined different activities that help cloud users to process on identified IS threats. This phase is very critical & technical and required due concentration of the threat solving team.4) Application The last act of this framework focuses on the use of the security metrics and threat severity levels by the decision makers. They evaluate the security and take suitable actions. This research determined the (Drive information security metrics) and (Security requirements) in phase 2 from standard and guide for guidance in metric development. The author was using the majority of this guidance as data security requirements in this project. The author has mentioned a set of international accepted frameworks; standards and guides are available for guidance in metrics development. IT Infrastructure Library (ITIL) and Control Objectives for Information and related Technology (CobiT) are renowned frameworks. International Organization for Standardization (ISO) has ISO/IEC 27002 information security and control

standards which also can be used to drive information security metrics. At present, SANS has also published an information security metrics guide which is very helpful for cloud users to drive information security metrics.

In 2012, Reference [3] presented an initial attempt to assess security requirements compliance of CSP by applying the Goal Question Metric (GQM) approach to quality measurement and defining a weighted scoring model for the assessment. The security goals and questions that address the goals are taken from CSA, Cloud Control Matrix (CCM) and CAIQ (Consensus Assessments Initiative Questionnaire) then transform such questions into more detailed ones and define metrics that help provide quantitative answers to the transformed questions based on evidence of security compliance provided by the cloud providers. The scoring is weighted by the quality of evidence, i.e. its compliance with the associated questions and its completeness. This research proposed scoring system architecture.

III. PROPOSED MODEL

Our Proposed model Fig. 5. measures the security compliance of the CSP semantics and matching their response to major international compliance guidance.

This model consists of three phases:

1) *Extracting ontology concepts of CC threat.*
2) *Extracting ontology concepts of CSP.*
3) *Matching Process between both ontology concepts.*

3.1 Phase One

The goal of this phase is to get the ontology concepts extractions for each CA Table 1.

3.1.1 Cloud Threats

In this work have addressed which CC threat can be measured. As mentioned earlier we studied the (Data Breaches Threat), CSA reported "TOP 10 CC Threats in 2013", and (Data Breaches Threat) was the 1st threat should be considered from CSPs and consumers. In this report can be defined the main parameters (CA) that cover this threat [9].

3.1.2 Cloud Control Area

This section addressed by two parts:

1- **Cloud Control Matrix (CCM):** This is designed to provide fundamental security principles to guide CSP and to assist prospective cloud customers in assessing the overall security risk of a CSP. The CCM provides a controls framework that gives a detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains [7].
2- **Consensus Assessments Initiative Questionnaire (CAIQ):** This effort is focused on providing industry-accepted ways to document what security controls exist in IaaS, PaaS, and SaaS offerings, providing security control transparency, and it's associated with CCM for more descriptions about CA with questions [6].

3.1.3 Compliance Guidance

This part represents a several international standard compliance guidance items that associated with each CA [7].

3.1.4 Miscellaneous Related Guidance

This part of several efforts has already taken place to offer guidance for cloud security. These include [39]:

1- Security Guidance for Critical Areas of Focus in CC V3.0: Published in 2011 presented security guidance for a number of areas in cloud computing; these include architecture, governance, traditional security, and virtualization [23].

2- Domain 12: Guidance for Identity & Access Management V2.1: Published in April 2010 discusses the major identity management functions as they relate to cloud computing. This work forms a cornerstone of the CSA's Trusted Cloud Initiative [22].

3- Cloud Computing: Information Assurance Framework: Published in November 2009. Presents a set of assurance criteria that address the risk of adopting cloud computing [5].

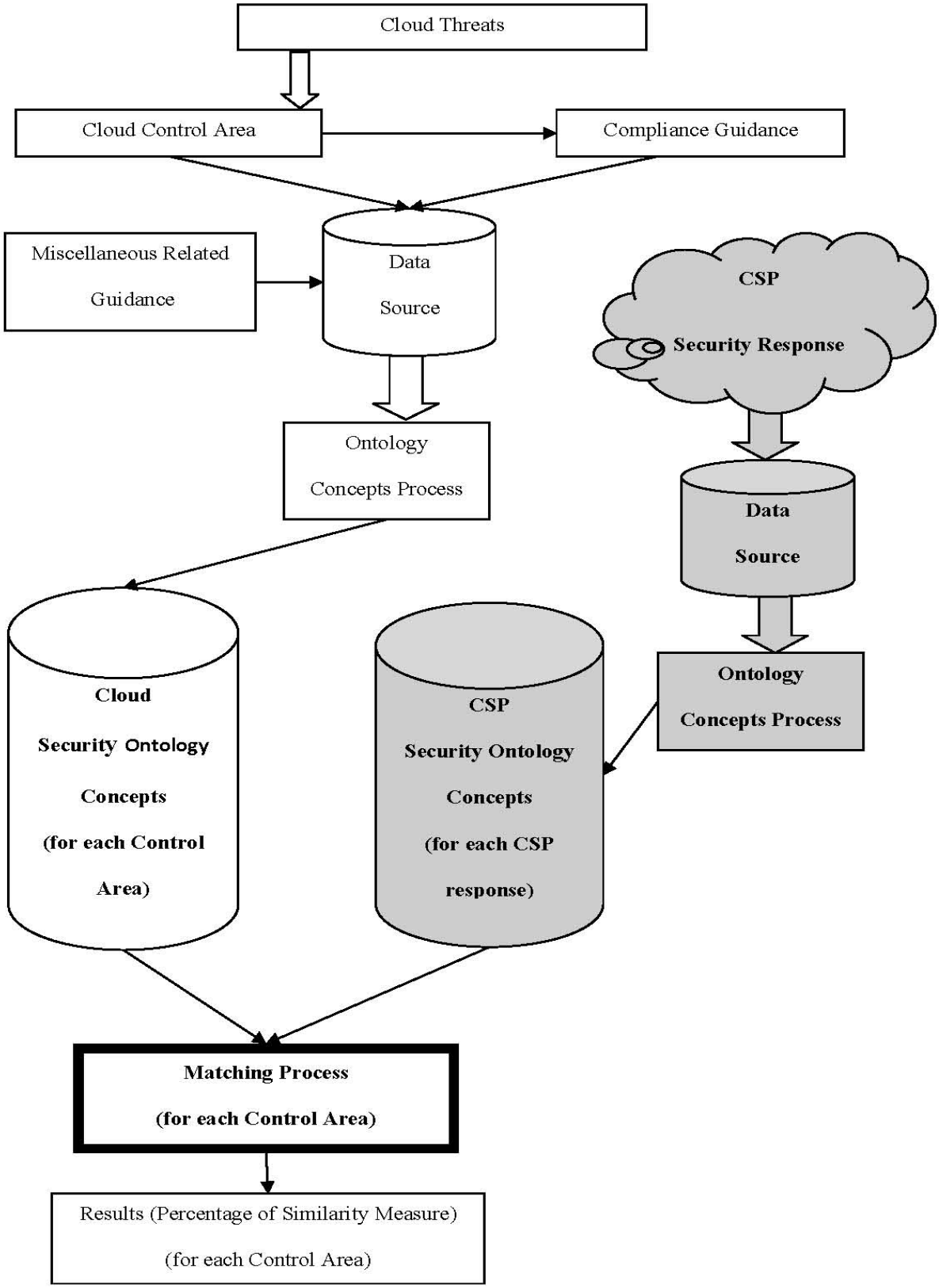

Fig. 5 Proposed Model to measures the security compliance of the CSP

4- The Federal CIO Council's Proposed Security Assessment and Authorization for U.S. Government Cloud Computing. The core importance of this document is that it adopts the NIST 800-53R3 security controls for cloud computing in low- and moderate-risk systems [11].

3.1.5 Data Source

It contains a set of the text files which are collected from the above documents.

3.1.6 Cloud Security Ontology Concepts (for each Control Area):

It contains the ontology concept extraction (by KAON TextToOnto Tool) [25] for each CA separately.

3.2 Phase Two

The goal of this part is to get the ontology concepts extractions for each CSPs response. We have taken 5 CSPs in our study.

3.2.1 CSP Security Response

It contains a different security response or actions of the CSPs for their compliances for each CA. We have taken 5 CSPs and searches to find 55 responses.

3.2.2 Data Source

It contains a set of the text files which are collected from the above section.

3.2.3 Cloud Security Ontology Concepts (for each Control Area):

It contains the ontology concept extraction (by KAON TextToOnto Tool) for each CSPs has a response for 11 CA separately, in our work we were extracted 55 state of ontology concepts totally.

3.3 Phase Three

This is the last component, it presents the matching process between the each output of the ontology concepts in part1 with the each output of the ontology concepts in phase two Fig. 6. then present the results.

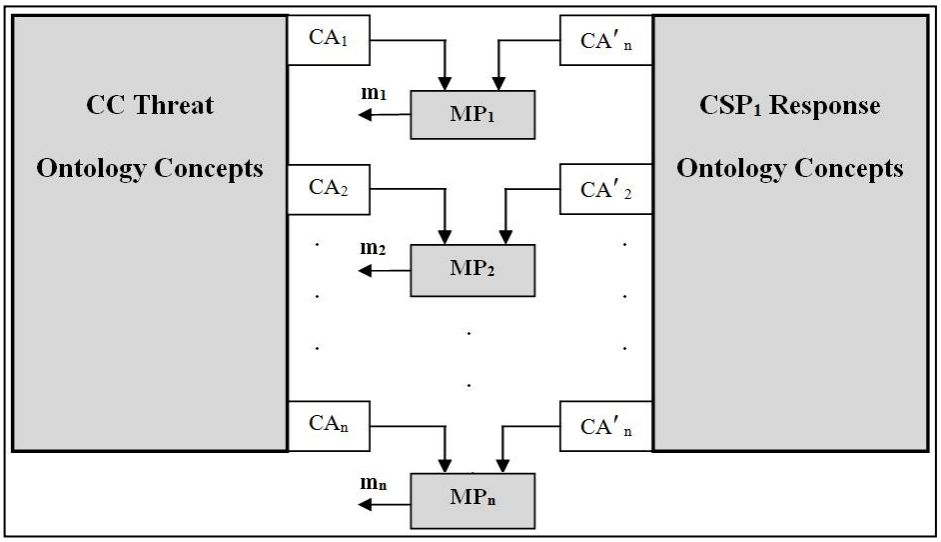

Fig. 6 Matching Concepts Process

The symbolic description of the (Figure 4.2) is :

CA_1 …. CA_n : Ontology concepts of CC Threat "Control Area CA"

CA'_1 …. CA'_n : Ontology concepts of CSP response for each CA

MP_1 …. MP_n : Semantic similarity measure between concepts of CA and CA′

$m_1 \ldots m_n$: Results (Total Measure Ratio)

n : Number of CA

IV. EXPERIMENTAL

4.1 Phase One – Collecting data and extracting ontology concepts of CC threat

We have collected data in details of the compliance items issued from major international standard organizations. These items are associated with the classification of the data breaches threat [7] as shown in Table 1. We arrange the data in a set of text file each CA separately; that means has collected (11) text files in order to use them in the next section [10] [14] [15] [28] [30].

TABLE IIIII
THE CLASSIFICATION FOR DATA BREACHES THREAT

Control Area	Control ID	Scope Applicability from International Standard Organizations				
		COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	PCI DSS v2.0
Data Governance - Retention Policy	DG-04	DS 4.1 DS 4.2 DS 4.5 DS 4.9 DS 11.6	45 CFR 164.308 (a)(7)(ii)(A) 45 CFR 164.310 (d)(2)(iv) 45 CFR 164.308(a)(7)(ii)(D) 45 CFR 164.316(b)(2)(i)	Clause 4.3.3 A.10.5.1 A.10.7.3	CP-2 CP-6 CP-7 CP-8 CP-9 SI-12 AU-11	3.1 3.1.1 3.2 9.9.1 9.5 9.6 10.7
Data Governance - Secure Disposal	DG-05	DS 11.4	45 CFR 164.310 (d)(2)(i) 45 CFR 164.310 (d)(2)(ii)	A.9.2.6 A.10.7.2	MP-6 PE-1	3.1.1 9.10 9.10.1 9.10.2 3.1
Data Governance - Non-Production Data	DG-06		45 CFR 164.308(a)(4)(ii)(B)	A.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	SA-11 CM-04	6.4.3
Data Governance - Information Leakage	DG-07	DS 11.6		A.10.6.2 A.12.5.4	AC-2 AC-3 AC-4 AC-6 AC-11 AU-13 PE-19 SC-28 SA-8 SI-7	1.2 6.5.5 11.1 11.2 11.3 11.4 A.1
Data Governance - Risk Assessments	DG-08	PO 9.1 PO 9.2 PO 9.4 DS 5.7	45 CFR 164.308(a)(1)(ii)(A) 45 CFR 164.308(a)(8)	Clause 4.2.1 c) & g) Clause 4.2.3 d) Clause 4.3.1 & 4.3.3 Clause 7.2 & 7.3 A.7.2 A.15.1.1 A.15.1.3	CA-3 RA-2 RA-3 MP-8 PM-9 SI-12	12.1 12.1.2

TABLE IIIII
THE CLASSIFICATION FOR DATA BREACHES THREAT

Control Area	Control ID	Scope Applicability from International Standard Organizations				
		COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	PCI DSS v2.0
				A.15.1.4		
Information Security - Encryption	IS-18	DS5.8 DS5.10 DS5.11	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312 (e)(1) 45 CFR 164.312 (e)(2)(ii)	A.10.6.1 A.10.8.3 A.10.8.4 A.10.9.2 A.10.9.3 A.12.3.1 A.15.1.3 A.15.1.4	AC-18 IA-3 IA-7 SC-7 SC-8 SC-9 SC-13 SC-16 SC-23 SI-8	2.1.1 3.4 3.4.1 4.1 4.1.1 4.2
Information Security - Encryption Key Management	IS-19	DS5.8	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312(e)(1)	Clause 4.3.3 A.10.7.3 A.12.3.2 A.15.1.6	SC-12 SC-13 SC-17 SC-28	3.4.1 3.5 3.5.1 3.5.2 3.6 3.6.1 3.6.2 3.6.3 3.6.4 3.6.5 3.6.6 3.6.7 3.6.8
Security Architecture - User ID Credentials	SA-02	DS5.3 DS5.4	45 CFR 164.308(a)(5)(ii)(c) 45 CFR 164.308 (a)(5)(ii)(D) 45 CFR 164.312 (a)(2)(i) 45 CFR 164.312 (a)(2)(iii) 45 CFR 164.312 (d)	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4 A.11.5.5	AC-1 AC-2 AC-3 AC-11 AU-2 AU-11 IA-1 IA-2 IA-5 IA-6 IA-8 SC-10	8.1 8.2 8.3 8.4 8.5 10.1 12.2 12.3.8

TABLE IIIII
THE CLASSIFICATION FOR DATA BREACHES THREAT

Control Area	Control ID	Scope Applicability from International Standard Organizations				
		COBIT 4.1	HIPAA / HITECH Act	ISO/IEC 27001-2005	NIST SP800-53 R3	PCI DSS v2.0
Security Architecture - Data Security / Integrity	SA-03	DS5.11		A.10.8.1 A.10.8.2 A.11.1.1 A.11.6.1 A.11.4.6 A.12.3.1 A.12.5.4 A.15.1.4	AC-1 AC-4 SC-1 SC-16	2.3 3.4.1 4.1 4.1.1 6.1 6.3.2a 6.5c 8.3 10.5.5 11.5
Security Architecture - Production / Non-Production Environments	SA-06	DS5.7		A.10.1.4 A.10.3.2 A.11.1.1 A.12.5.1 A.12.5.2 A.12.5.3	SC-2	6.4.1 6.4.2
Security Architecture - Remote User Multi-Factor Authentication	SA-07			A.11.1.1 A.11.4.1 A.11.4.2 A.11.4.6 A.11.7.1	AC-17 AC-20 IA-1 IA-2 MA-4	8.3

We need to extract the ontology concepts for each CA of the data breaches threat; in order to do this task should be considered about the information knowledge. We have used KAON TextToOnto tool in order to extract the ontology concepts each CA from the text file as mentioned above. Table 3. showing the (57) ontology concept for the first CA “Retention Policy”. Also; the ontology concepts of the remaining CA(s) have been extracted Table 4.

TABLE III
ONTOLOGY CONCEPTS FOR (CA′1) "RETENTION POLICY"

No.	Concepts	No.	Concepts	No.	Concepts	No.	Concepts
1	access	16	documentation	31	organization	46	risk
2	area	17	example	32	paper	47	security
3	assessment	18	facility	33	part	48	service
4	audit	19	framework	34	period	49	site
5	availability	20	guidance	35	plan	50	software
6	backup	21	handle	36	point	51	storage
7	business	22	identification	37	policy	52	store
8	capability	23	impact	38	process	53	supplement
9	contingency	24	incident	39	protection	54	support
10	control	25	information	40	record	55	system
11	critic	26	infrastructure	41	recovery	56	test
12	data	27	integrity	42	response	57	time
13	disaster	28	list	43	restoration		
14	disposal	29	loss	44	resumption		
15	disruption	30	management	45	retention		

TABLE IV
NO. OF ONTOLOGY CONCEPTS FOR (11) CONTROL AREA (CA)

Control Area (CA)	No. of Ontology Concepts
DG-04- Retention Policy	57
DG-05 - Secure Disposal	23
DG-06 - Non-Production Data	32
DG-07 - Information Leakage	46
DG-08 - Risk Assessments	61
IS-18 - Encryption	56
IS-19 - Encryption Key Management	46
SA-02 - User ID Credentials	52
SA-03 - Data Security/Integrity	59
SA-06 - Production/Non-Production Environments	25
SA-07 - Remote User Multi-Factor Authentication	39

4.2 Phase Tow – Collecting data and extracting ontology concepts of CSP

Our research has been included five providers: Amazon Web Service (AWS), Windows Azure, License12, Krescendo, and CloudSigm. These providers are chosen based on the availability level of data describes security issues, different service, size (small, medium and large), also AWS and Windows CSPs are certified from different international organizations and included the top 100 CSPs ranking (Cloud Times and TalkinCloud); the last three CSPs are out on those ranking web sites. During collection data procedure we associate any terms or items necessary to be defined by more information in the Text file as possible.
We extracted ontology concepts for a CSP response for each CA. Practically, we by using the TextToOnto KAON tool Table 5.

TABLE V
ONTOLOGY CONCEPTS OF CSPS FOR "RETENTION POLICY" CONTROL AREA

DG-04 - Retention Policy					
No.	AWS	Azure	License12	Krescendo	CloudSigma
1	availability	backup	addition	access	completion
2	backup	business	data	agency	distribution
3	business	center	internality	business	enhancement
4	capacity	customer	regularity	client	industry
5	data	data	standard	compliance	management
6	database	disaster	time	data	material
7	enforcement	domain		government	notification
8	instance	event		information	
9	law	example		request	
10	option	fault		retention	
11	period	help		service	
12	production	information		solution	
13	recovery	infrastructure		specification	
14	relation	loss		system	
15	retention	machine		view	
16	service	platform			
17	storage	program			
18	time	recovery			
19		redundancy			
20		replication			
21		restoration			
22		retention			
23		review			
24		service			
25		state			
26		storage			
27		tolerance			
28		validation			

4.3 Phase Three – Matching Process

We applied Semantic Similarity Measure (SSM) for matching between concepts by using WS4J Tool [40]. We have used similarity measure developed by Lin [23] and it is intended to be useful in nearly any environment [38] with accepted correction value is (0.834) and it is range (0-1) [16].

We used the below equation In order to compute the total measure ratio (m1...m11):

$$\text{Total Measure} = \frac{\text{No. of Concepts by Lin Similarity Mesure}}{\text{No. of Concepts of CA'1}} \quad \text{..... (1)}$$

$$\text{Total Measure} = \frac{15}{18}$$

$$\text{Total Measure} = 0.833$$

- We applied the above equation (1) for all CSPs, and compare it with human judges (professors, doctors, and practitioners we asked them during our study) Table 6.

TABLE VI
AWS MEASURE RATIO

No.	CA	Human Ratio	Total Measure Ratio ($m_1..m_{11}$)	No. of Concepts by SSM	No. of Concepts
1	DG-04	0.950	0.833	15	18
2	DG-05	0.900	0.857	18	21
3	DG-06	0.850	0.750	12	16
4	DG-07	0.850	0.760	19	25
5	DG-08	0.950	0.800	12	15
6	IS-18	0.900	0.764	13	17
7	IS-19	0.900	0.772	17	22
8	SA-02	0.850	0.785	11	14
9	SA-03	0.900	0.846	11	13
10	SA-06	0.950	0.913	21	23
11	SA-07	0.950	0.750	21	28
	Average	0.905	0.803		

We have computed the total error among human judge's ratio and total measure ratio (m1 .. m11) by using Mean Square Error (MSE):

$$\text{MES} = \frac{\sum_{n}^{1}(\text{Human Ratio} - \text{Total Measure Ratio})^2}{n} \times 100 \qquad \text{..... (2)}$$

Table 7. present the error percentage using MES for all CSPs of (11 CAs)

TABLE VII
MEASURE RATIO FOR ALL CSPS (11 CA)

Threat Domain	Error Percentage (%)				
	AWS	Azure	License12	Krescendo	CloudSigma
Data Breaches	1.268	1.164	0.480	1.135	1.776
Average Error	1.165 %				

We note that the error percentage of (License12) is (0.480%) about the half percentage from other CSPs due its security compliance's for (8) CAs. Therefore, we have computed the error percentage for the (8) participates CA.

Table 8. present the error percentage using MES for all CSPs of (8 CAs).

TABLE VIII
MEASURE RATIO FOR ALL CSPS (8 CA)

Threat Domain	Error Percentage (%)				
	AWS	Azure	License12	Krescendo	CloudSigma
Data Breaches	0.861	0.797	0.480	1.090	1.195
Average Error	0.885 %				

Table 9. presents the measurement comparison between human and our measure for 8 CA (Total Measure).

TABLE IX
MEASURE RATIO FOR ALL CSPS (8 CA)

Threat Domain	Average (%)									
	AWS		Azure		License12		Krescendo		CloudSigma	
	Human	SSM	Human	SSM	Human	SSM	Human	SSM	Human	SSM
Data Breaches	90.5	80.3	84.5	74.6	56.3	52.1	55.5	49.9	41.4	41.5

V. CONCLUSIONS

After matching process in phase 3 of our proposed model; completed the following results are founded:

1. Our approach average error in our approach (0.885 %) is acceptable when compare with other [3].
2. The reliability of the semantic measure result depends on the security information that is provided from CSP.
3. CSPs do not disclose more about his security issues.
4. The highest score to security compliance is for CSP (AWS and Azure), due they has certified from the major international standard organizations (Table 9).
5. Number of ontology concepts assigns the level of the security compliance.
6. Uncertified CSP has a limitation for their security response.

VI. FUTURE WORK

We would like to suggest a few ideas for future study:

1. Possibility to use our approach to measure other CC threats (like Account Hijacking, Data Loss ... etc) semantically.
2. Build full otology domain for each CA as security requirements.
3. Providing full coverage for all ontology domains, to let the measure be more accurate and reliable.
4. Develop a graphics user interface to present the results.

REFERENCES

[1] Almorsy M., Grundy J., & Müller, I. (2010). *An Analysis Of The Cloud Computing Security Problem*. In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30 th Nov 2010, [Online]. Available: http://www.cs.auckland.ac.nz/~john-g/papers/cloud2010_1.pdf

[2] Baker, W., Hutton, A., Hylender, C. D., Pamula, J., Porter, C., & Spitler, M. (2011). *Data Breach Investigations Report*. Verizon RISK Team. [Online].Available: www.verizonbusiness.com/resources/reports/rp_databreach-investigations-report-2011_en_xg. pdf

[3] Bhensook, N., & Senivongse, T. (2012). *An Assessment Of Security Requirements Compliance Of Cloud Providers*. In Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference 520-525, Doi: 10.1109/CloudCom.2012.6427484

[4] Boss, G., Malladi, P., Quan, D., Legregni, L., & Hall, H. (2007*). Cloud Computing. Ibm* white paper, Version, 1. [Online]. Available: http://download.boulder.ibm.com/ibmdl/pub/software/dw/wes/hipods/Cloud_computing_wp_final_8Oct.pdf

[5] Catteddu, D., & Hogben, G. (2009). *Cloud Computing Information Assurance Framework*. European Network and Information Security Agency (ENISA).

[6] Cloud Security Alliance (CSA), 2011, *Consensus Assessments Initiative Questionnaire (CAIQ) V1.1*. https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v1-1/

[7] Cloud Security Alliance (CSA), 2013. *Cloud Control Matrix V3 (CCM*), [Online]. Available:https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3

[8] Cloud Security Alliance, 2010, *Top Threatsto Cloud Computing V1.0*. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[9] Cloud Security Alliance, 2013, *Cloud Computing Top Threats In 2013* .[Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

[10] *Control Objectives For Information And Related Technology (Cobit)*, 4rd Edition, IT Governance Institute, 2007, www.itgi.org

[11] Council, I. A. (2012). *Federal Risk And Authorization Management Program* (FedRAMP).

[12] Curran, k., Carlin, S., & Adams, M. (2011). *Security Issues In Cloud Computing*. Elixir Network Engg, 38, 4069-4072, Doi: 10.4018/978-1-4666-0957-0.ch014.

[13] Fenz, S. (2010). *Ontology-Based Generation Of It-Security Metrics*. Proceedings of the 2010 ACM Symposium on Applied Computing, 1833-1839.

[14] *Hipaa. Health Insurance Portability And Accountability* Act Of 1996.

[15] International Organization for Standardization (ISO) (2005b) ISO/IEC 27001 *Information Technology- Security Techniques- Information Security Management Systems Requirements, Iso/Iec 27001:2005(E).* ISO Copyright Office. Published in Switzerland.

[16] Jarmasz, M. (2003). *Roget's Thesaurus As A Lexical Resource For Natural Language Processing*. arXiv preprint arXiv:1204.0140.

[17] Jiang, R. *From Ontology To Semantic Similarity: Calculation Of Ontology-Based Semantic Similarity*. The Scientific World Journal, 2013.

[18] Jing, X., & Jian-jun, Z. (2010). *A Brief Survey On The Security Model Of Cloud Computing*. In Distributed Computing and Applications to Business Engineering and Science (DCABES), 2010 Ninth International Symposium, 475-478, Doi: 10.1109/DCABES.2010.103

[19] Julisch, K. (2009). *Security Compliance: The Next Frontier In Security Research*, In Proceedings of the 2008 workshop on New security paradigms. 71-74, doi:10.1145/1595676.1595687.

[20] Kandukuri, B. R., Paturi, V. R., & Rakshit, A. (2009). *Cloud Security Issues. In Services Computing*, 2009. SCC'09. IEEE International Conference, 517-520, Doi:10.1109/SCC.2009.84.

[21] Kumar, V., Swetha, M., Muneshwara, M. S., & Prakash, S. (2012). *Cloud Computing: Towards Case Study Of Data Security Mechanism.* Int. J. Adv. Technol. Eng. Res, 2 (4).

[22] Kumaraswamy, S., Lakshminarayanan, S., Stein, M. R. J., & Wilson, Y. (2010). Domain 12: *Guidance For Identity & Access Management V2. 1*. Cloud Security Alliance, (On-Line), available: http://www. cloudsecurityalliance. org/guidance/csaguide-dom12-v2, 10.

[23] Lin, D. (1998, July). *An Information-Theoretic Definition Of Similarity*. In ICML (Vol. 98, pp. 296-304).

[24] Luna, J., Ghani, H., Germanus, D., & Suri, N. (2011). *A Security Metrics Framework For The Cloud*. In Proc. of the INSTICC Internation Conference on Security and Cryptography, 245-250.

[25] Maedche, A., & Volz, R. (2001). *The Ontology Extraction & Maintenance Framework Text-To-Onto.* In Proc. Workshop on Integrating Data Mining and Knowledge Management, USA, 1-12.

[26] Mell, P., & Grance, T. (2011). *The NIST Definition Of Cloud Computing*, English, special publication, Us Department Of Commerce, 800 (145), 7.

[27] Nagwani, N., & Verma, S. (2011). *A Frequent Term And Semantic Similarity Based Single Document Text Summarization Algorithm*, International Journal of Computer Applications. 17 (2), 36-40, Doi: 10.1109/ICTKE.2012.6152388.

[28] *Nist Recommended Security Controls*- FISMA. 2009. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf

[29] Pal, D. G. (2012). *A Novel Open Security Framework For Cloud Computing*, International Journal of Cloud Computing and Services Science (IJ-CLOSER). 1 (2), 45-52.

[30] PCI DSS. *Requirements and Security Assessment Procedures*,2009. . [Online]. Available:https://www. pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2. Pdf
[31] Putri, N. R., & Mganga, M. C. (2011). *Enhancing Information Security In Cloud Computing Services Using Sla Based Metrics* (Doctoral dissertation). Master's thesis: Blekinge Institute of Technology.
[32] *Security Guidance For Critical Areas Of Focus In CC V3.0* (Cloud Security Alliance, 2011).
[33] Shuanglin, R. (2012), *Data Security Policy In The Cloud Computing*. In Computer Science & Education (ICCSE), 2012 7th International Conference, 222-225, Doi: 10.1109/ICCSE.2012.6295062
[34] Tariq, M. I. (2012). Towards *Information Security Metrics Framework For Cloud Computing*. International Journal of Cloud Computing and Services Science (IJ-CLOSER), 1 (4), 209-217.
[35] The Wikipedia website. [Online]. Available: http://www. Wikipedia.org/
[36] Townsend, M. (2009). *Managing A Security Program In A Cloud Computing Environment*. In 2009 Information Security Curriculum Development Conference, 128-133, Doi: 10.1145/1940976.1941001
[37] Ullah, K. W. (2012). *Automated Security Compliance Tool For The Cloud*, (Doctoral dissertation). Norwegian university of science and technology, Norwegian University, Trondheim.
[38] Warin, M. (2004). *Using Wordnet And Semantic Similarity To Disambiguate An Ontology*. Retrieved January, 25, 2008, (On-Line), available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.95.9729&rep=rep1&type=pdf
[39] Winkler, V. J. (2011). *Securing The Cloud: Cloud Computer Security Techniques And Tactics*. Elsevier.
[40] Wordnet Similarity For Java (WS4J) [Online]. Available: http://ws4jdemo.appspot.com
[41] Yildiz, M., Abawajy, J., Ercan, T., & Bernoth, A. (2009). *A Layered Security Approach For Cloud Computing Infrastructure*. In Pervasive Systems, Algorithms, and Networks (ISPAN), 10th International Symposium ,763-767, Doi: 10.1109/I-SPAN.2009.157

