IJETAE
EXPLORING RESEARCH AND INNOVATIONS

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 6, June 2015)

Mitigation Techniques to Security Flaws in Cloud Computing

Emmanuel Adinkrah[1], J.B Hayfron-Acquah[2], Joseph Kobina Panford[3]

[1]*Department of Computer Science, Christian Service University College, Kumasi, Ghana*
[2,3]*Department of Computer Science, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana*

***Abstract*— The advent of Cloud computing signifies a paradigm shift in traditional computing systems. It is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. Organizations have expressed concern about critical issues (such as security) that exist with the widespread implementation of cloud computing. These types of concerns originate from the fact that data is stored remotely from the customer's location. In this paper, two research methodologies are adopted and utilized. These are Systematic Literature Review, Survey and interviews with various users working in the Cloud Computing environment. Conclusively, some eight (8) security challenges were identified along with its mitigation techniques. The most measured attribute is confidentiality (31%) followed by integrity (24%) and availability (19%). The impact of identified mitigation techniques is mainly on security (30%), followed by performance (22%) and efficiency (17%). Furthermore, two of such security threats; Data Loss/Leakage and Insecure Application Programming Interfaces are duly reviewed and mitigations proposed in this paper.**

***Keywords*— Cloud Computing, Security, SaaS, IaaS, PaaS, Elasticity, API, Data Loss/Leakage.**

I. INTRODUCTION

A. Background Study

Cloud computing is envisioned as the next-generation architecture of IT Enterprise [1], which aims to consolidate the economic utility model with the evolutionary development of many existing approaches and computing technologies, including distributed applications, services, and information infrastructures. Via cloud computing, users can uniformly access distributed resources on the Internet on demand [2]. Cloud computing also refers to both the applications delivered as services over the Internet and the hardware and software in the datacenters that provide those services. Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructure. In cloud environments, several kinds of virtual machines are hosted on the same physical server as infrastructure. In cloud, costumers must only pay for what they use and do not have to pay for local resources, which they need such as storage or infrastructure.

Nowadays, there are three types of cloud environments: Public, Private, and Hybrid clouds. A public cloud is standard model which providers make several resources, such as applications and storage, available to the public. Public cloud services may be free or not. In public clouds, there are running applications setups externally by large service providers and thus offers some benefits over private clouds. Private Cloud refers to internal services of a business that is not available to the public. Essentially Private clouds are a marketing term for an architecture that provides hosted services to particular group of people behind a firewall. Hybrid cloud is an environment that a company provides and controls some resources internally and has some others for public use. It can be defined as a combination of private and public clouds. In this type, the cloud provider has a service that has a private cloud part, which is only accessible by certified staff and protected by firewalls and a public cloud environment which external users can gain access. There are three major types of service in the cloud environment: SaaS, PaaS, and laaS [3]. In the cloud-computing ecosystem, similar to every proposed technology, there are issues of security that needs to be addressed. Some of these security issues are:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service and Traffic Hijacking
- Unknown Risk Profile

In this paper, two of these security issues are discussed and proposed mitigation steps provided. These are Insecure Application Programming Interfaces (APIs) and Data Loss/Leakage. Insecure Application Programming Interfaces grants third-party access by exposing the applications to Application Programming Interfaces (APIs), and as such organizations may be required to relinquish their credentials to third parties in order to enable their usage. Here, a risk that relates to anonymous access or improper authentication will lead to application security issues. Through the insecure APIs, intrusion risk are bigger in cloud environment which adds complexity or blocks visibility to network-based systems [4].

The cause of most application security issues has been attributed to bad application development practices. Such cloud environments also use applications, which are built for in-house deployments therefore, suffer from many bugs. Thus, the impact posed by insecure APIs cannot be underestimated. Secondly, in the case of Data Loss/Leakage threat (DLT), it has been one of the biggest fears that most of the organizations face today. Innately, when transitioning to a cloud there are two changes that happen to a customer's data. First, the data will be stored away from the customer's local machine. Secondly, the data will move from a single-tenant to a multi-tenant environment. During this data transition, there is some loss of data that is known as data leakage.

In a private cloud, the customer has direct control over the whole infrastructure. In a hybrid cloud, if the cloud service is IaaS, the client could implement Data Loss/Leakage Prevention agents to ensure the loss is prevented or in some cases minimized.

B. *Statement of the Problem*

It is without any doubt that cloud computing is a breakthrough technology that will continue to unleash new efficiencies and advantages to enterprises. It removes infrastructure and capital expense as a barrier to entry and allows start-up organizations to scale up cheaply and rapidly. On the other hand, enterprises face limitations in using the cloud for high-performance and mission-critical applications such as ERP. However, there is a major concern about critical issues such as security that exist with the widespread implementation of cloud computing. These concerns originate from the fact that data is stored remotely from the customer’s location and thus prompting some of the security requirements and issues that involve data, application and virtualization in the cloud computing.

II. THE PURPOSE OF THE STUDY

The purpose of this paper is to find out the benefits and drawbacks in regards with data security and data availability in a cloud based ERP; thus how the use of Cloud Computing for the implementation and management of their information system can affect the organization. Finally concluding the factors in terms of data security and data availability, enterprises should keep in mind while adopting Cloud Computing for the effective and efficient use of their information system. An overview of the purpose of this research can be summarized as:

i. To identify techniques and/or approaches in mitigating security challenges in the ERP Cloud enterprise.

III. RELATED WORKS

A. *Cloud Threat Models*

The origin of threats towards data within the cloud is described together with two threat models based upon a specific lifecycle. Thus, irrespective of the nature of the attacks, it will appear to function within a certain type of threat model. The first model represents a user-centric view, the other a Cloud Service Provider point of view. By considering the Cloud as a remote storage system i.e. NAS, one can take existing threat models [5] that look towards the area of remote storage and adapt them, as necessary, for the Cloud. This provides a discussion of two threat models for remote storage systems. The first, classifies threats based upon their effect upon the four ‘classical’ security requirements of confidentiality, integrity, authorization and availability. The second classifies threats according to how the threats affect data during its lifecycle. A threat model based upon the data lifecycle allows for such a model to be constructed. The purpose of a threat model is to classify the different threats and vulnerabilities into groups so that they can be resolved accordingly.

B. *Origin of Threats*

The origin of threats to data can be divided into the following categories; Outsiders are entities that exist outside of the system and attempt to subvert/circumvent the security infrastructure of the service or masquerade as a legitimate service to ensnare users. Their motivation will stem from simple curiosity or from malice. Insiders are more serious threats, which originate from current or past employees of the Cloud Service Providers. Employees will have intricate knowledge of the actual infrastructure including that of security and as part of their remit may have had direct access to the data itself or through other means. Similar to insiders their motive may be out of curiosity or of malice. Natural Threats although both insiders and outsiders can induce ‘errors’ within the infrastructure, other errors can occur naturally from the software itself or from hardware failure. For example, when Google pushed a software update to Google Docs, the software malfunction changed the sharing settings of several users’ documents to include those with whom the affected users had share documents with before.

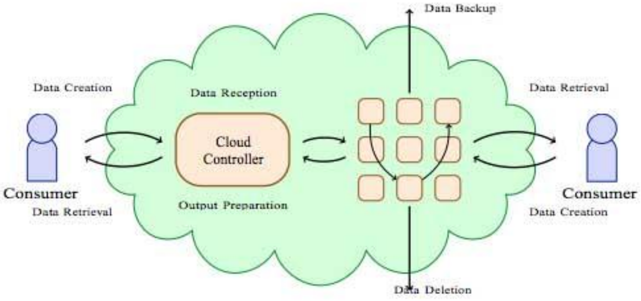


Figure 1: Data lifecycle threat model for the Cloud.

Consumers interacting with both the Cloud Controller and also with the virtualized resources will also be presented with the appearance of a single entity. The data (including the virtual machine) may also be replicated on various virtualized resources and also among different physical machines. By combining this data center model with that of the data lifecycle model for remote storage systems a threat model for the cloud can be produced. Figure 1 summarizes this new model. The difference between this model and the existing one is that the single data store has been replaced by virtual resources. This increases the number of places within the model where these stages can exist.

IV. USER-CENTRIC MODEL

The overall threat model represents an omniscient narrator's view of the cloud; they see and are privy to all aspects. However, one must also consider the user's point of view. They are not aware of all aspects of the internal workings of the cloud. Thus, one can also present a user centric threat model that uses as a basis the clients' viewpoint. In this model the client views the cloud as a single entity.

The more astute reader will notice that this is reminiscent of the original data lifecycle model. Data goes in the cloud, data comes out the cloud, data gets archived, and data is deleted. The user is not aware per se that the data could migrate between nodes within the cloud. Figure 2 illustrates this user centric model

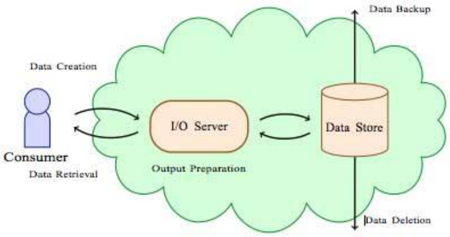


Figure 2: The Data Lifecycle Threat Model for Service Users.

V. METHODOLOGY

The primary consideration in choosing a methodology is the research questions that can be identified within three parameters, which are; explanatory, descriptive or exploratory [6, 7]. The primary consideration was the research questions. The intent was to use Christian Service University College, Ghana (Cloud Computing user) and Google Cloud Computing Service (Cloud Computing provider) as case studies. The results were analyzed on a specific framework or theory to check the benefits or drawbacks for enterprises adapting Cloud Computing in regards with data security. Christian Service University College was ideal case study because they had adopted and were using Cloud Computing in their organization. It was prudent not to choose more enterprises for the case study because of the lack of resources. Another reason for choosing CSUC was, because it was easier to get approval for the case study and source information from the relevant people. In relation to this study, the initial step taken was to create a study protocol. The goal of the study protocol was to collect data from a single case or a single respondent. It shows the step by step of how the data was collected and help anticipate the problems. The study protocols included the context and the perspective of the specific study, the field procedure, and case study questions. It helped to focus on the right questions related with the enterprise and their use of Cloud Computing and their awareness of the security implications, to get to right conclusions. The qualitative approach adopted, the aim was to get both the overall understanding of the information system of enterprise and Cloud Computing along with the perceived benefits and security drawbacks related to them, hence, the most appropriate method was to conduct semi-structured interview.

The first interview was conducted in CSUC focusing on the Cloud Computing and the cost effects on ERPs. This helped to formulate an interview guide. The questionnaire started with introductory questions followed by general view of Cloud Computing. The second interview with the same employees of CSUC focused on security issues of Cloud Computing for enterprises. In this interview, it started with the general questions about security and following with the specific questions like implementation of security, data connection encryption, TLS, security for different models of Cloud Computing, and governance issues. Questions around the benefits offered to ERPs by Cloud Computing included centralized data, audit and effective updates was formulated for use. The third interview was done with the cloud provider Hapaweb Solutions, a licensed partner of Google Ghana and it focused on the provider's perspective of Cloud Computing. The interview was more of a general interview about security effects on ERPs present in the real market. Once the interviews were completed the next stage was to convert the interview from oral speech to text. The interviews were recorded with an Apple IPAD, which was a convenient means of recording and transcribing voice notes [7]. Transcription reliability and validity is an important issue to take care of. Adherence to the reliability of quality shall be to transcribe same interview from oral speech to text and then compare with accordingly [8].

VI. Research Design

There are a number of research designs that were considered to generate reliable data and to meet research objectives irrespective of whether the research was qualitative or quantitative in nature. These are experimental design, longitudinal design, cross-sectional design and case study design. This divides these designs into fixed and flexible research designs [9]. The participants were ideally randomly assigned to different conditions, and variables of interest were measured. The intent was to control the other variables in other to avoid interference or casualty. As stated earlier, case study design was the most fitting to this research and was applied appropriately. Case study as an empirical inquiry was chosen because it allowed focus to be placed on the research topic. It is in these settings that data was gathered and utilized.

VII. Sampling Techniques

The sampling of the participants at CSUC was carried out using simple random sampling where only the key personnel were chosen using purposive sampling since these were key informants and possess the required information for the study.

VIII. Study Sample

The sample size of the study was thirty (30) due to the small number of staff interested in this research. The staff consisted of I.T personnel, End users and management members who were chosen at random.

IX. Response Rate

During the data collection, out of the 30 interviews/questionnaire, which were distributed to the field, 27 useable questionnaires were returned giving a response rate of 90%.

X. Data Analysis Technique

The goal of the case study analyses was to make a very precise description of the case and its setting. In this case, effects of Cloud Computing in enterprises, the security threats and its mitigation techniques. All the data collected, were used to establish an outline, concerning each step in the processes described above. The direct interpretation was used to select a precise instance, a single one, and try to find out the meaning of it, without cross checking or having multiple sources available to help [10]. In this paper, this process helped to establish a stronger meaning to the study, when placed back together all the textual data that was found. An algorithmic approach to undertake the study was by identifying the issues in Cloud Computing and its security threats and mitigation approaches in ERPs, which was the primary purpose of the study.

XI. Implementation, Testing And Evaluation

The proposed framework was called the "Beacon", an online student management system that consisted of four interactive components. These components were the

i. User Interface (Client),
ii. The database server,
iii. The Application Programming Interfaces (APIs)
iv. The Cloud Computing Platform.

The standard Java technologies were adopted and was run on Google's scalable web application infrastructure. The Java environment provides a Java 6 JVM, a Java Servlets interface, and support for standard interfaces to the App Engine scalable data store and services, such as JDO, JPA, Java Mail, and JCache. The App Engine runs Java applications using the Java 6 virtual machine (JVM). The App Engine Java SDK includes tools for testing application, uploading your application files, and downloading log data. The SDK also includes a component for Apache Ant to simplify tasks common to App Engine projects. The development server runs the application on a local computer for development and testing. The development server can also generate configuration for data store indexes based on the queries the app performs during testing.

XII. System Requirement

i. A complete Java 6 runtime environment in a secure sandbox environment.
ii. Based on common Java web technology standards, including servlets and WARs, JDO and JPA, java.net, JavaMail and JCache.
iii. A plugin for the Eclipse IDE makes project creation, testing and deployment a snap.
iv. Supports other languages that compile to the JVM or use JVM-based interpreters, such as JRuby, JavaScript (Rhino), and Scala.
v. Microsoft. NET frameworks 4.0
vi. Google API runtime source codes
vii. Microsoft SQL Server 2012 with Client Access Licenses (CALs)

XIII. Functions Of The Interactive Components

A. Users

- Manages student records such as creating and editing student's details, academic records.
- Manages examination records such as entry of scores, deletion and updates.
- Manages student semester registration, deferment processes.
- Manage the verification, issuance of academic transcripts.

XIV. Database

The Cloud database application operated on the MS SQL 2008 server R2. It served to provide the following functions:

i. Verify user account, username and password of the users.
ii. Verify access level rights and privileges.
iii. Record date of transactions across all levels
iv. Record all student information (Bio-Data, Academic Records etc.)
v. Verify and generate academic transcripts, attestation letters.

XV. System Design Of The Current Model

Many scholars have proposed cloud-based architectures particularly for ERPs [11] defined the Cloud architecture for ERPs as a stack of the following layers: Hardware, Visualization, IaaS, PaaS and SaaS. The stack was illustrated as a pyramid, with the layer "Hardware" being the base and SaaS being the top. Using their proposed architecture, they designed the conceptual framework of (Figure 3) that aims to enhance productivity, efficiency, transparency, participation and collaboration of traditional ERPs. This system was designed on Client/Server architecture that was developed on the windows and network groups. This system included three main parts, which are the User Interface module, the Server module and the Google API module. The purpose of the Google API module was to facilitate the processing of data parsed by the client to be stored in the Google cloud. The server stores all transactions in the database, which are related to the transaction details.

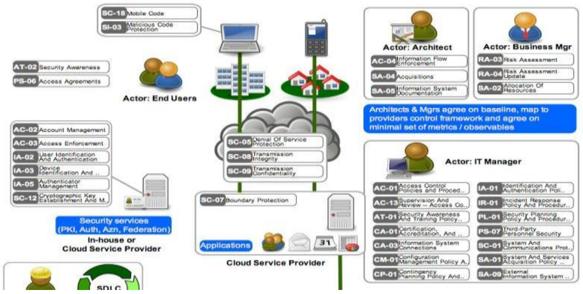

SC-18 Mobile Code
SI-03 Malicious Code Protection
AT-02 Security Awareness
PS-06 Access Agreements
Actor: End Users
AC-02 Account Management
AC-03 Access Enforcement
IA-02 User Identification And Authentication
IA-03 Device Identification And ..
IA-05 Authenticator Management
SC-12 Cryptographic Key Establishment And M..
Security services (PKI, Auth, Azn, Federation)
In-house or Cloud Service Provider
SDLC
SC-05 Denial Of Service Protection
SC-08 Transmission Integrity
SC-09 Transmission Confidentiality
SC-07 Boundary Protection
Applications
31
Cloud Service Provider
Actor: Architect
AC-04 Information Flow Enforcement
SA-04 Acquisitions
SA-05 Information System Documentation
Actor: Business Mgr
RA-03 Risk Assessment
RA-04 Risk Assessment Update
SA-02 Allocation Of Resources
Architects & Mgrs agree on baseline, map to providers control framework and agree on minimal set of metrics / observables
Actor: IT Manager
AC-01 Access Control Policies and Proced..
AC-13 Supervision And Review -- Access Co..
AT-01 Security Awareness And Training Policy..
CA-01 Certification, Accreditation, And ..
CA-03 Information System Connections
CM-01 Configuration Management Policy A..
CP-01 Contingency Planning Policy And..
IA-01 Identification And Authentication Poli..
IR-01 Incident Response Policy And Procedur..
PL-01 Security Planning Policy And Procedur..
PS-07 Third-Party Personnel Security
SC-01 System And Communications Prot..
SA-01 System And Services Acquisition Policy ..
SA-09 External Information System ..

Figure 3: A module of the system

XVI. Proposed Framework

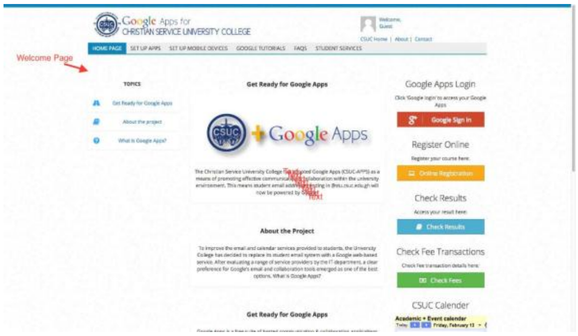
The proposed framework was called CSUC Online Registration Portal (Beacon) which consists of three (3) components that are established in the cloud (SAAS) and they are:

- Database Server (MS SQL 2008)
- Google Application Programming Interface
- Graphical User Interface (GUI)

Each of these components utilized a certain level of security as necessary to ensure data protection, privacy and consistency is always guaranteed.

XVII. MODEL OF THE PROPOSED SYSTEM

The proposed system will operate on a more secure platform in the cloud.



The Christian Service University College [illegible] Google Apps (CSUC-APPS) as a means of promoting effective communica[illegible] collaboration within the university environment. This means student email add[illegible] in @stu.csuc.edu.gh will now be powered by Google

About the Project

To improve the email and calendar services provided to students, the University College has decided to replace its student email system with a Google web-based service. After evaluating a range of service providers by the IT department, a clear preference for Google's email and collaboration tools emerged as one of the best options. What is Google Apps?

Get Ready for Google Apps

Figure 4: "Beacon" Welcome Page

The Welcome Page shown in Figure 4: allows users to make a selection of what they intend to do on the portal.

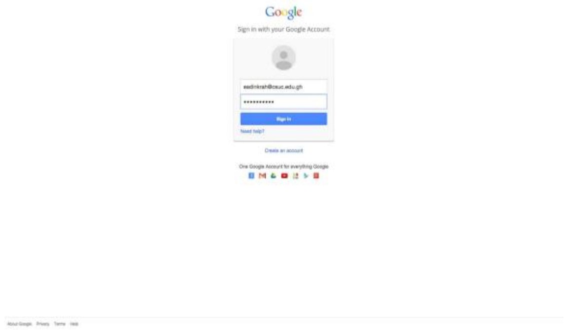
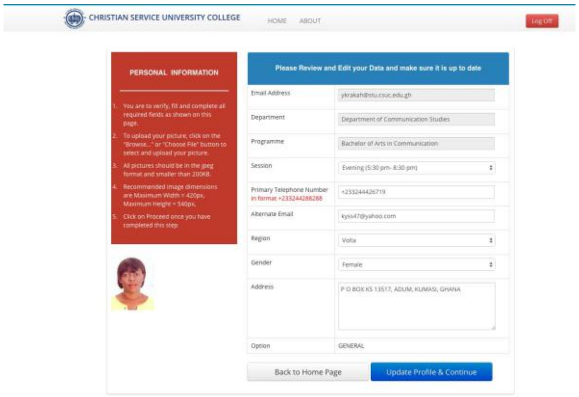


Figure 5: The Google Apps Login Page

The Google Apps Login Page as shown in Figure 4 interface presented the same interface a Google email user will use to login. However, because of the Application Programming Interface (API) that was embedded into the system, the user authentication for portal users will be done against the MSSQL Server with Google Synchronization coming into effect. This ensured only valid users gain access into the system.


CHRISTIAN SERVICE UNIVERSITY COLLEGE
HOME
ABOUT
Log Off
Back to Home Page
Update Profile & Continue

PERSONAL INFORMATION

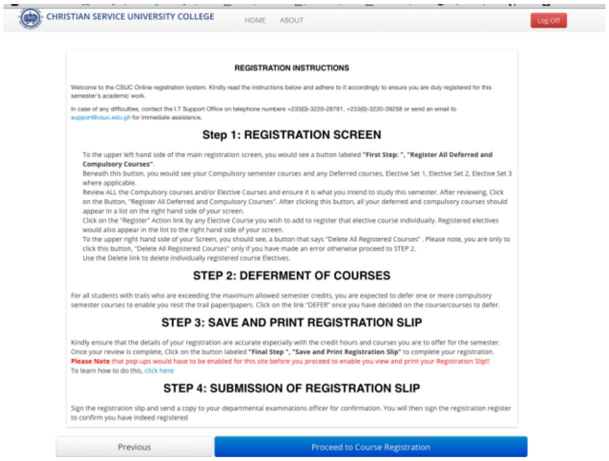
1. You are to verify, fill and complete all required fields as shown on this page.
2. To upload your picture, click on the "Browse..." or "Choose File" button to select and upload your picture.
3. All pictures should be in the jpeg format and smaller than 200KB.
4. Recommended image dimensions are Maximum Width = 420px, Maximum Height = 540px,
5. Click on Proceed once you have completed this step

Please Review and Edit your Data and make sure it is up to date

Email Address	ykrakah@stu.csuc.edu.gh
Department	Department of Communication Studies
Programme	Bachelor of Arts in Communication
Session	Evening (5:30 pm- 8:30 pm)
Primary Telephone Number in format +233244288288	+233244426719
Alternate Email	kyss47@yahoo.com
Region	Volta
Gender	Female
Address	P O BOX KS 13517, ADUM, KUMASI, GHANA
Option	GENERAL

Figure 5: The Student Profile Page

The Student Profile page as shown in figure 5 illustrates the various personal information that the student must update in order to be able to proceed to the next step. Some of the information requested was session of student, the mobile phone number of the student, the region of the student, Postal Address and Option in the course of the study. Once this information was updated, the student could continue with the process.


CHRISTIAN SERVICE UNIVERSITY COLLEGE
HOME
ABOUT
Log Off
Previous
Proceed to Course Registration

REGISTRATION INSTRUCTIONS

Welcome to the CSUC Online registration system. Kindly read the instructions below and adhere to it accordingly to ensure you are duly registered for this semester's academic work.

In case of any difficulties, contact the I.T Support Office on telephone numbers +233(0)-3220-28781, +233(0)-3220-39258 or send an email to support@csuc.edu.gh for immediate assistance.

Step 1: REGISTRATION SCREEN

To the upper left hand side of the main registration screen, you would see a button labeled **"First Step: ", "Register All Deferred and Compulsory Courses"**.
Beneath this button, you would see your Compulsory semester courses and any Deferred courses, Elective Set 1, Elective Set 2, Elective Set 3 where applicable.
Review ALL the Compulsory courses and/or Elective Courses and ensure it is what you intend to study this semester. After reviewing, Click on the Button, "Register All Deferred and Compulsory Courses". After clicking this button, all your deferred and compulsory courses should appear in a list on the right hand side of your screen.
Click on the "Register" Action link by any Elective Course you wish to add to register that elective course individually. Registered electives would also appear in the list to the right hand side of your screen.
To the upper right hand side of your Screen, you should see, a button that says "Delete All Registered Courses" . Please note, you are only to click this button, "Delete All Registered Courses" only if you have made an error otherwise proceed to STEP 2.
Use the Delete link to delete individually registered course Electives.

STEP 2: DEFERMENT OF COURSES

For all students with trails who are exceeding the maximum allowed semester credits, you are expected to defer one or more compulsory semester courses to enable you resit the trail paper/papers. Click on the link "DEFER" once you have decided on the course/courses to defer.

STEP 3: SAVE AND PRINT REGISTRATION SLIP

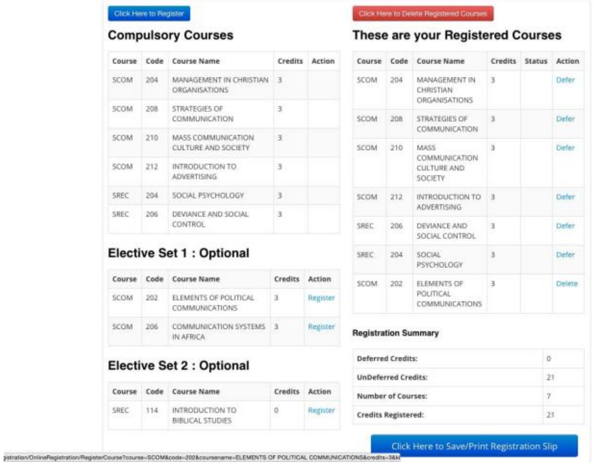
Kindly ensure that the details of your registration are accurate especially with the credit hours and courses you are to offer for the semester.
Once your review is complete, Click on the button labeled **"Final Step ", "Save and Print Registration Slip"** to complete your registration.
Please Note that pop-ups would have to be enabled for this site before you proceed to enable you view and print your Registration Slip!!
To learn how to do this, click here

STEP 4: SUBMISSION OF REGISTRATION SLIP

Sign the registration slip and send a copy to your departmental examinations officer for confirmation. You will then sign the registration register to confirm you have indeed registered

Figure 6: Instructional Information For Authorized Student

Figure 6 shows the interface that displays the relevant information for an authorized student to be able to register successfully. It provided a detailed, step-by-step guide as to how to complete the entire registration. After reading the information, students are expected to click on "Proceed to Registration" to move to the next stage.


Click Here to Register
Click Here to Delete Registered Courses
Click Here to Save/Print Registration Slip
gistration/OnlineRegistration/RegisterCourse?course=SCOM&code=202&coursename=ELEMENTS OF POLITICAL COMMUNICATIONS&credits=3&k

Compulsory Courses

Course	Code	Course Name	Credits	Action
SCOM	204	MANAGEMENT IN CHRISTIAN ORGANISATIONS	3	
SCOM	208	STRATEGIES OF COMMUNICATION	3	
SCOM	210	MASS COMMUNICATION CULTURE AND SOCIETY	3	
SCOM	212	INTRODUCTION TO ADVERTISING	3	
SREC	204	SOCIAL PSYCHOLOGY	3	
SREC	206	DEVIANCE AND SOCIAL CONTROL	3	

Elective Set 1 : Optional

Course	Code	Course Name	Credits	Action
SCOM	202	ELEMENTS OF POLITICAL COMMUNICATIONS	3	Register
SCOM	206	COMMUNICATION SYSTEMS IN AFRICA	3	Register

Elective Set 2 : Optional

Course	Code	Course Name	Credits	Action
SREC	114	INTRODUCTION TO BIBLICAL STUDIES	0	Register

These are your Registered Courses

Course	Code	Course Name	Credits	Status	Action
SCOM	204	MANAGEMENT IN CHRISTIAN ORGANISATIONS	3		Defer
SCOM	208	STRATEGIES OF COMMUNICATION	3		Defer
SCOM	210	MASS COMMUNICATION CULTURE AND SOCIETY	3		Defer
SCOM	212	INTRODUCTION TO ADVERTISING	3		Defer
SREC	206	DEVIANCE AND SOCIAL CONTROL	3		Defer
SREC	204	SOCIAL PSYCHOLOGY	3		Defer
SCOM	202	ELEMENTS OF POLITICAL COMMUNICATIONS	3		Delete

Registration Summary

Deferred Credits:	0
UnDeferred Credits:	21
Number of Courses:	7
Credits Registered:	21

Figure 7: Main Registration Interface for Students

Figure 7 shows the main registration page for students. In this user interface, students are expected to select their appropriate courses for the semester. Once this is done, they complete the registration by saving and printing the registration slip.

XVIII. Testing

In testing this cloud application, errors can occur at any stage in the development cycle. During this test cycle, the application is executed with a set of test cases, and the output of the test cases is evaluated to determine if the program is performing as expected.

XIX. Testing Strategy

The testing of the cloud application was also done using the following strategy:

Component Testing: Each component that made up the application was tested. These included the students' records, the Google Application Programming Interface (API), the Registration Portal.

Integrated Testing: The various modules of the application were integrated and tested to ensure the correct interworking of the components (Database server, Google API, Cloud Application).

Validation Testing: The integrated cloud application was tested to ensure that it works correctly in a pseudo-live environment.

XX. Testing Priorities

During the testing of the application, the following qualities were tested in order of priorities.

- *Functionality* –Whether the required functions are available and working as expected.
- *Usability* – How user-friendly and intuitive the application is.
- *Security*- How well protected was the application and data that is in the cloud.
- *Performance* – Whether the application response times are within acceptable limits.

XXI. Evaluation

A. Overview Of Case Study Participants

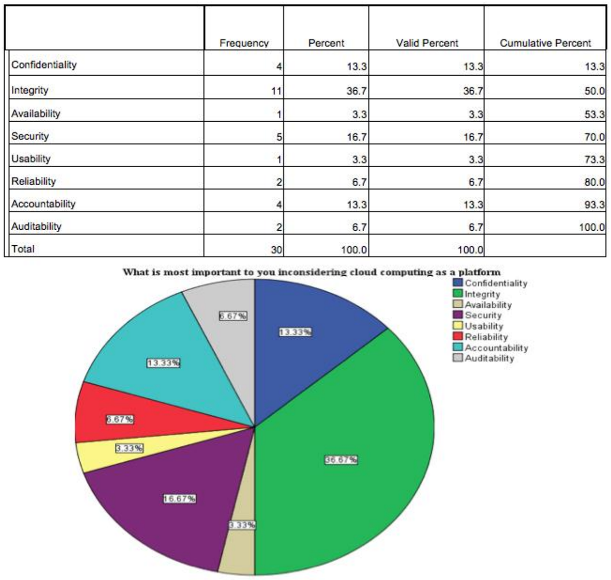
The respondents who completed the questionnaires were selected on basis of their roles at CSUC. One of the key areas in which scholars have focused, is cases of governments or agencies that have already used cloud computing but using CSUC which is an educational organization provides very insightful findings. In total, thirty partially and completed responses from the real time survey was obtained. However, many did not have relevant experience in Cloud Computing and IT security but showed keen interest. The adopted experts had experience from 1 to 10 years.

B. Findings - Reported Challenges

In the part of the Survey, a total of 14 Security challenges, which were possible to be faced in the future of Cloud Computing were identified. This was summarized as future security challenges based on the opinions from experts. The results are displayed in the table 1:

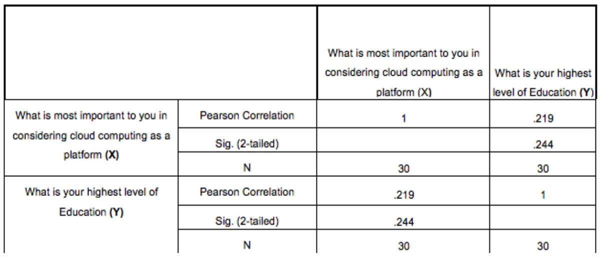
Table 1:
List of Cloud Based Reported Challenges

1. Hypervisor viruses	**8.** Risk of multiple Cloud tenants
2. Abuse and nefarious use of Cloud Computing	**9.**Insecure application programming interfaces
3. Service and traffic hijacking	**10.** Business intelligence – Business confidential will be handled by IT companies all over the world. No one knows who is accessing user company's data.
4. Data ownership – When data is transferred to the Cloud it is important for many organizations to be assured of the continued control of the data, i.e. their ownership should never be challenged.	**11.** Privacy – Personal information about many people will be handled by IT companies all over the world. No one will know who is accessing user data.
5. Malicious insiders	**12.**Shared technology vulnerabilities
6. Transparency – Using Cloud services has to be as simple as traditional solutions. The compromised attributes are confidentiality, security, availability and integrity.	**13.** Availability – The availability must be at least as high as for traditional solutions.
7. Interception point	**14.** Smart phone data slinging



	Frequency	Percent	Valid Percent	Cumulative Percent
Confidentiality	4	13.3	13.3	13.3
Integrity	11	36.7	36.7	50.0
Availability	1	3.3	3.3	53.3
Security	5	16.7	16.7	70.0
Usability	1	3.3	3.3	73.3
Reliability	2	6.7	6.7	80.0
Accountability	4	13.3	13.3	93.3
Auditability	2	6.7	6.7	100.0
Total	30	100.0	100.0	

Figure 8: Frequency of Compromised attributes



		What is most important to you in considering cloud computing as a platform (X)	What is your highest level of Education (Y)
What is most important to you in considering cloud computing as a platform (X)	Pearson Correlation	1	.219
	Sig. (2-tailed)		.244
	N	30	30
What is your highest level of Education (Y)	Pearson Correlation	.219	1
	Sig. (2-tailed)	.244	
	N	30	30

Figure 9: List of Compromised attributes

C. Correlational And Regressional Analysis

A STATISTICAL SOFTWARE TOOL, STATISTICAL PACKAGE FOR THE SOCIAL SCIENCES (SPSS) WAS USED FOR THE DATA ANALYSIS**. The correlation and regression analysis of both variables (x and y) are presented in Tables 7 and 8. The highest level of education is indicated as Y and the most important in considering cloud computing as a platform is indicated as X.**

The following hypotheses were tested as the correlation and regression analyses were conducted.

Null Hypotheses (H0): There is no statistically significant correlation between x and y.

Alternative Hypotheses (Ha): There is statistically significant correlation between x and y.

Table 2:
Pearson Correlation

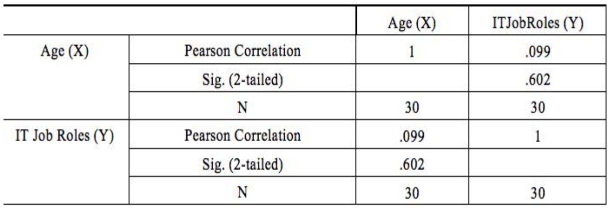
		X	Y
X	Pearson Correlation	1	.219
	Sig. (2-tailed)		.244
	N	30	30
Y	Pearson Correlation	.219	1
	Sig. (2-tailed)	.244	
	N	30	30

From Table 2, the value r = 0.219 indicates a few things.

- *Direction:* Firstly, this is a positive correlation coefficient. This means there is a positive low or weak correlation between y and x since 0<r<0.5, where r is the correlation coefficient. As x increases, y increases.

- Based on the correlation result, the factors to be considered in choosing a cloud-computing platform is strong. This is because there is low or weak correlation between x and y as the correlation coefficient is between 0 and 0.5, thus knowing x does not give enough prediction of y and vice versa.

XXII. Correlation Between Age (X) And Job Title (Y) Variables



		Age (X)	ITJobRoles (Y)
Age (X)	Pearson Correlation	1	.099
	Sig. (2-tailed)		.602
	N	30	30
IT Job Roles (Y)	Pearson Correlation	.099	1
	Sig. (2-tailed)	.602	
	N	30	30

Figure 10: Correlation between Age (X) and Job Title (Y) variables

From Figure 10, the value of r = 0.099 which is indicative of a trend.

- *Direction:* There is a positive correlation coefficient, which implies there is a positive low or weak correlation between x and y since 0<r<0.5, where r is the correlation coefficient. As x increases, y increases.
- Based on the correlation coefficient which is between 0 and 0.5, thus knowing the age (x) of a user does not give enough prediction of y (job role) and vice versa. In its practicality, the age and job role of a user has no effect on the choice of what the user considers as a high priority compromised attribute.

XXIII. Findings - Suggested Mitigation Techniques

From the analysis of results from survey using SPSS software, nine mitigation techniques were identified to address the security challenges. The major security techniques that are used in the current world are:

SSL (Secure Socket Layer) Encryption: Encryption between browser and web server. It usually provides enough security from the workstation to the browser. The use of SSL does not require Cloud service provider for any functionality. It is all in how you have defined your website. It was easily available as it was very inexpensive. All Cloud customers should require encrypted communication. Optical fiber is another tool, since fibers are harder to manipulate than electrical cables.

VPN (Virtual Private Network): VPNs are most commonly used for home based or mobile applications. When users connect to the internet from home or any public place like airport, hotel etc., then he will be signed into his VPN and get secure communication. Many Cloud providers offer VPNs to cover the area from the workstation in user facility to user connection to the Internet and across the internet.

IPSec (Internet Protocol Security): IPSec is a prominent appearance of VPN, usually used between facilities where there is a large amount of traffic. In the case of Cloud, Cloud service provider will define and usually facilitate the IPSec device to install user network where it connects to the internet and to facilitate high speed encryption and decryption without keeping workload on servers.

A proper use of encryption can give good protection against eaves dropping. Traffic analysis is harder, but on the other hand, not only that many need protection against this kind of threat.

Intrusion Detection system and Service management API (SMAPI)

The above mentioned mitigation techniques have strong impact on the Performance, Security, Efficiency, QoS, Privacy and Access control of Cloud Computing. The defined mitigation techniques somehow improve the overall services in Cloud Computing environment. The result is shown in figure 10

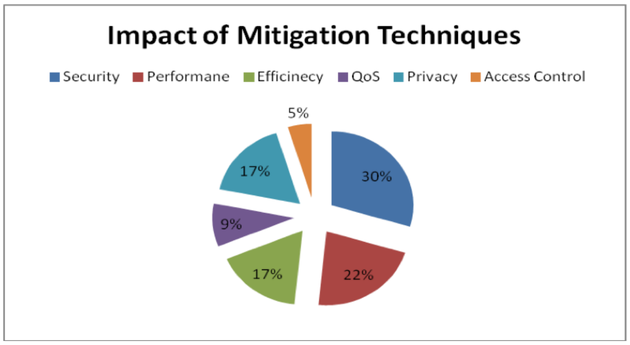


Figure 11: Impact of mitigation techniques

Also, a summarized suggested practices from experts to mitigate future challenges to be faced in Cloud Computing. The summary includes:

- Increased efforts in risk management – One should have a better risk awareness in order to take proper risks.
- Standardized security methods and solutions.

- Increased efforts to mitigate harmful code; Legal responsibility, and increased security measurements at levels of objects and elements of objects.
- Analyze the security model of Cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Implement strong API access control.

XXIV. Conclusion And Future Work

In the future, the people will access and share their software applications through online and access information by using the remote server networks instead of depending on primary tools and information hosted in their personal computers because of flexibility in Cloud Computing. The security issues in Cloud Computing are always one of the main research topics for researchers and developers to investigate the appropriate solutions. From the perspective of this paper, it is suggested that it is prudent to find optimum and appropriate security solutions for the specific services in the Cloud. There is a scope to propose the guidelines to overcome the future challenges like physical security, espionage, transparency, data ownership, hypervisor viruses and malicious insiders in Cloud security. Thus, to concentrate more on specific areas like regulatory and compliance issues, jurisdiction laws, etc.

References

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, A., and Zaharia, M. (2009). Above the clouds: A berkeley view of cloud.

[2] Boss, G., Malladi, P., Quan, D., Legregni, L., Hall, H. (2007), Cloud Computing. ww.ibm.com/developerworks/websphere/zones/hipods/. Retrieved on 20th May, 2010.

[3] Bolin, Jason S. Use Case Analysis for Adopting Cloud Computing in Army Test and Evaluation. Naval Postgraduate School Master's Thesis, September 2010, at:http://edocs.nps.edu/npspubs/scholarly/theses/2010/Sep/10Sep_Bolin.pdf (accessed October 24, 2010).

[4] Catteddu, D. and Hogben, G. (2009). Cloud Computing: benefits, risks and recommendations for information security. Communications in Computer and Information Science. 72(1, 17).

[5] Cloud Computing – Demystifying SaaS, PaaS and IaaS by Cloud tweaks. Available at: http://www.cloudtweaks.com/2010/05/cloud-computing-demystifying-saas-paas-and-iaas/ [Visited 05-04-2011]

[6] Linthicum, David. "Three Cloud Computing Mistakes You Can Avoid Today." MISAsia, March 12, 2010, at: http://mis-asia.com/cio_focus/technology/3-cloud-computing- mistakes-you-can-avoid-today (accessed September 10, 2010).

[7] Lynch, M. (2008) The Cloud Wars: $100+ billion at stake. Merrill Lynch research note, May 2008. Retrieved May 15, 2010 from http://web2.sys-con.com/node/604936.

[8] Mathisen, Eystein. (may 31, 2011) 'Security challenges and solutions in Cloud Computing', Digital Ecosystems and Technologies Conference (DEST), 5th IEEE International Conference, 208-212.

[9] Tie Fang Wang, Baosheng Ye. (July 2010) 'Study on enhancing performance of cloud trust model with family gene technology', 3rd IEEE International conf. on Computer Science and Information Technology (ICCSIT), 122-126.

[10] Wood K, Pereira E. (Nov.2010) 'An Investigation into Cloud Configuration and Security', 2010 International Conference for Internet Technology and Secured Transactions, 1-6.

[11] Zetter, Kim. "Vulnerabilities Allow Attacker to Impersonate Any Website." *Wired.com*, July29, 2009, at: http://www.wired.com/threatlevel/2009/07/kaminsky/ (accessed July 23, 2010).