A Resiliency Framework for an Enterprise Cloud

Victor Chang[1], Muthu Ramachandran[1], Yulin Yao[2], Yen-Hung Kuo[3], Chung-Sheng Li[4]

1. School of Computing, Creative Technologies and Engineering,
Leeds Beckett University, Leeds, UK.
2. Independent Researcher, Southampton, UK
3. Data Analytics Technology & Applications, Institute for Information Industry, Taiwan, R.O.C.
4. IBM Thomas J. Watson Research Center, Yorktown Heights, NY 10598, USA

Correspondance e-mail: V.I.Chang@leedsbeckett.ac.uk

***Abstract*— This paper presents a systematic approach to develop a resilient software system which can be developed as emerging services and analytics for resiliency. While using the resiliency as a good example for enterprise cloud security, all resilient characteristics should be blended together to produce greater impacts. A framework, Cloud Computing Adoption Framework (CCAF), is presented in details. CCAF has four major types of emerging services and each one has been explained in details with regard to the individual function and how each one can be integrated. CCAF is an architectural framework that blends software resilience, service components and guidelines together and provides real case studies to produce greater impacts to the organizations adopting Cloud Computing and security. CCAF provides business alignments and provides agility, efficiency and integration for business competitive edge. In order to validate user requirements and system designs, a large scale survey has been conducted with detailed analysis provided for each major question. We present our discussion and conclude that the use of CCAF framework can illustrate software resilience and security improvement for enterprise security. CCAF framework itself is validated as an emerging service for Enterprise Cloud Computing with analytics showing survey analysis.**

Keywords- Software resiliency; Resilient software for Enterprise Cloud; Cloud computing Adoption Framework (CCAF); Cloud security and software engineering best practice

1. INTRODUCTION

Software Engineering has established techniques, methods, and technology over two decades. However, the concept of resiliency has not been exploited well and software security related attacks and how systems are capable of withstanding such an attack remains research challenge. Some of the software security issues are caused by the direct attributes such as applications, user interface, and communication tools. Current applications are being developed and delivered where security has been patched as aftermath. Early commercial developers have tackled security problems using firewalls (at the application level), penetration testing, and patch management (Curphey and Arawo, 2006; McGraw, 2006). Building resilient software system will help to build trust for users and communities, protect data centres for critical applications such as medical systems and other critical systems (Friedman and West, 2010; Rajkumar et al., 2010). Software resiliency needs to be defined and identified as we start identifying requirements for software systems. It is relevant to Cloud Computing as an Emerging Service that provides data analysis of outputs.

There is a growing demand and pervasiveness for the majority of people to be involved directly or indirectly with fast growing information warfare, cybercrime, cyber-terrorism, identify theft, spam, and other various threats. It is hence important to understand the security concerns starting from requirements, design, and testing. Therefore, we can actually build in security instead of batching security afterwards. McGraw (2006) asserts that *a central and critical aspect of the computer security problem is a software problem*. This book defines *software security engineering as a discipline which considers capturing and modelling for security, design for security, adopting best practices, testing for security, managing, and educating software security to all stakeholders*.

Software engineering has well established framework of methods, techniques, rich processes that can address small to very large scale products and organizations (CMM, CMMi, SPICE, etc.), and technologies (UML modeling, CASE tools, and CAST tools, etc.). Software Engineering has also been well established quality,

reusability, reliability models, methods and numerous lists of other techniques. The so called "lities" of software engineering has been contributed as part of quality attributes which are known as Quality, Testability, Maintainability, Security, Reliability and Reusability. These attributes cannot be just added on to the system as they have to be built in from early part of the lifecycle stages (Gillies, 2011). It is a typical software development lifecycle include starting from requirements engineering (RE), software specification, software & architectural design, software development (coding), software testing, and maintenance. Security has become highly important attribute since the development of online based applications. Software project management has well established techniques and breadth of knowledge including global development (due to the emergence of internet revolution and people skills across the globe), cost reduction techniques, risk management techniques, and others. Now a day, most of the current systems are web enabled and hence security needs to be achieved right from beginning: need to be identified, captured, designed, developed and tested (Ramachandran, 2008; Ramachandran, 2012; Ramachandran and de Carvalho 2010; Gillies, 2011). Hence, a consolidated research is required into interplay between social engineering and software engineering for developing a secured software system, with aims to define and identify software resiliency for a software system to build trust, security, and integrity. All these can help organizations achieve enterprise security since their services are more robust and resilient to hacking, errors and faults. To present our research in developing resilient software systems, a framework is proposed with the rationale and the details of the software components illustrated. Surveys have been conducted with 400 valid samples. Collective user requirements are used as the input for system design and development of the framework, so that the framework can be demonstrated as an emerging service and analytics to validate its resilience and robustness.

The breakdown of this paper is as follows. Section 2 describes the related work for building a resilient software framework. Section 3 presents research methodology with an overview of the framework, Cloud Computing Adoption Framework (CCAF) and the resilient component services. Section 4 explains the survey results and how they can be used for the framework development. Section 5 proposes the framework with the four major services and the details in each component of each service. Section 6 explains how CCAF framework can be used as a business resilient framework to provide the competitive edge. Section 7 justifies the collective user requirements for the CCAF development with the rationale explained for summary of comments given by the respondents. Section 8 describes the target met and designed by the CCAF framework to consolidate why CCAF is an emerging service. Section 9 sums up Conclusion and future work.

2. RELATED WORK

This section describes the related work with regard to the attack methods, since a comprehensive understanding can help design and improve guidelines for a security framework of cyber security incidents between February and August of 2011 compiled by X-Force of IBM, which include Amazon's loss of data in 2011 and 2012, and the problems with Elastic Load Balancing services in 2013 and RSA's hacked data and services (Li, 2014). Among all security incidents in the previous five years, the most severe incident is the attack on RSA during March 2011. This incident involves what is known as ***Five-layered of Advanced Persistent Threat*** (APT), and often includes the following five phases over an extended period of time:

1. **Social Engineering**: Initially, spear phishing emails were sent over a two-day period to small groups of employees with RSA. The email subject line read *2011 Recruitment Plan*, was from beyond.com – an HR partner firm of RSA. The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability. One of the RSA employees clicked the attachment from junk mail.
2. **Back Door**: The malware installed a customized remote administration tool known as Poison Ivy RAT to allow external control of the PC or server, and set up the tool in a reverse-connect mode.
3. **Moving Laterally**: The malware first harvested access credentials from the compromised users (user, domain admin, and service accounts), then performed privilege escalation on non-administrative users in the targeted systems, and then moved on to gain access to key high value targets.
4. **Data Gathering**: Attacker behind the malware in the RSA case established access to staging servers at key aggregation points.

5. **Exfiltrate**: The attacker then used FTP to transfer many password-protected RAR files from the RSA file server to an outside staging server on an external, compromised machine at a hosting provider. Once the transfer completed, the footprints were wiped clean making it impossible to trace back to the attackers.

2.1 A resilient software framework

A resilient software framework is required to ensure that all services are safe, robust and secure. All the components and layers within the emerging services can be useful for organizations to adopt. In exceptional circumstances such as unauthorized access and hacking, the resilient service can withstand all these five commonly attacking approaches. To ensure that a resilient framework is in place, all the essential characteristics in security services are required, which includes the followings:

- **Identification** is a basic and the first process of establishing and distinguishing amongst person/user and admin ids, a program/process/another computer ids, and data connections and communications.
- **Privacy** is the key to maintaining the success of cloud computing and its impact on sharing information for social networking and teamwork on a specific project. This can be maintained by allowing users to choose when and what they wish to share in addition to allowing encryption and decryption facilities when they need to protect specific information/data/media contents.
- **Integrity** is defined as a process of maintaining consistency of actions, communications, values, methods, measures, principles, expectations, and outcomes. Ethical values are important for cloud service providers to protect integrity of cloud users' data with honesty, truthfulness and accuracy at all time.
- **Durability** is also known as, persistency of user actions and services in use should include sessions and multiple sessions.

The other important aspects are as follows.

- **Confidentiality, Privacy and Trust** – These are well known basic attributes of digital security such as authentication and authorization of information as well protecting privacy and trust.
- **Cloud service security** – This includes security on all its services such as SaaS, PaaS, and IaaS. This is the key area of attention needed for achieving cloud security.
- **Big data security** – This category is again paramount to sustaining cloud technology. This includes protecting and recovering planning for cloud data and service centers. It is also important to secure data in transactions.
- **Physical protection of cloud assets** – This category belongs to protecting cloud centers and its assets.

2.2 Building in resiliency

This section describes software resiliency and success factors for building resiliency for enterprise security. IT and Software Engineering communities rarely understand the concept of resiliency, which has been a characteristic of living organisms (Holling, 1996). For example, ecological resilience is common in biology. In order for any species to survive under hard conditions, organisms may partly change or evolve their habits and behaviors. Over a period of time, the mutation happens. Similarly, when a stress or shock happens at some point in life, people tend to respond by protecting against such a shock or even a fall into the ground. Therefore, we need to understand the concept of resilience from other area such as building communities, social sciences, disaster management systems, nursing and so on. Torrence Resilience Institute (TRI, 2009) defines as a Latin verb "resilire", meaning to rebound or recoil. They classify resilience into a number of areas such as human individuals, ecological, organizational, community, economy, etc. As shown in Figure 1, TRI (2009) defines characteristics of resilience in dual directions. Careful planning is thus required to ensure that all the software strategies and services can work together rather than work apart.

Figure 1: Characteristics of resilience

Software has been the key element of any applications, devices, and platforms which provide us with the required services and functionalities. High integrity, safety and resiliency of systems have been paramount as this directly leads to securing safety of people. Currently with the increase of computer related crime and fraud such as security and online crimes is doubling every year. This causes huge loss (data, money, business amongst other forms of losses) and stress to people, businesses, government sectors, and organizations. Software is everywhere and hence the flaws due to software errors. Our earlier research has demonstrated a systematic development and reuse of software components with Build-In Security (BIS) (Ramachandran, 2008; 2010; 2012). A number of methodologies for agile software development and product line engineering have been developed. Our current research includes requirements engineering methods for software security, best practice guidelines for secured software systems implementation, and we have developed an online security assessment model which has been used by a number of software companies to identify their current security measures. The proposed project aims to investigate how to build-in resiliency, safety, and security of software systems (Merkow and Raghavan, 2010; Gabrys, 2011; Ramachandran 2012):

- Define and classify software resiliency for building software systems;
- Automated assessment for how to build-in security for software resilience;
- A model and a set of best practice guidelines for organization to choose how to avoid disasters (such as data recovery plan and attacks by hacking and virus) and to cope with computer related crimes such as identity fraud and phishing;
- A framework for assessment and improvement model for IT systems security;
- A learning process model for helping people to cope with new technologies;
- A knowledge-based e-commerce best practices to help government and organization to safe guard against computer related crimes which has been reported to have doubling each year;
- To identify key methods and techniques to study social engineering for software security;
- Knowledge based best practices on internet security for individuals and organizations;
- To build a system for software resilience assurance with cyber security best practices;
- To build a model for software trustworthiness;
- To investigate resilient process model for building software systems;
- Develop methods and strategies to build-in software security;
- Software safety techniques for high integrity systems (medical, transport, and defense systems) with resilience to avoid human disasters and
- Autonomic recovery systems supporting software resilience (intrinsic resiliency of the software system itself as well as the resiliency of the software imparts upon other components).

The overall aim of this project is to build a system for automated assessment and improvement for any resilient software systems and to build a framework for security. Each work package will be based on the number of objectives as identified.

3. RESEARCH METHODOLOGY FOR RESILIENT COMPUTING

This section presents research methodology which will be based on eliciting requirements (agile based methods combining ethnography and social science research techniques) from various stakeholders. Such techniques will involve ethnography and social science research techniques to capture requirements and to understand current social and economic impacts of modern technology and its disasters that it creates quite often recently. The methodology will require to build a system that can assess and improve cyber security and trustworthy of existing and new systems alike. Additionally, evaluation includes user evaluation and metrics on cyber security and trustworthiness of systems.

The methodology is based on system design and results from large scale surveys. The system design should ensure each selected security solution can follow the best practice approach and is robust enough for all different types of tests. The integration between different technologies can successfully be delivered and implemented in the in-house environments such as simulations to ensure that all the rest results can be validated. User requirements have to be collected and transformed into the development of the CCAF. Hence, the large scale survey results will be analysed in Section 4, the framework of system design and how it can fit into a business resilient framework will be presented in Sections 5 and 6 respectively, and the evaluation of the collective user requirements will be conducted in Section 7.

Before explaining details of methodology steps in order, following two subsections are going to give an overview introduction of the Cloud Computing Adoption Framework (CCAF) and the resilient component services as preliminary knowledge. Resiliency is a design characteristics of a system which cannot be just be added to a system instead it should be build-in from requirements identification. Hence, CCAF plays an important role in identifying and developing for resilient system.

3.1 Cloud Computing Adoption Framework Overview

Cloud Computing Adoption Framework (CCAF), an architectural framework with software components and services, is developed to meet the requirements mentioned above. CCAF also blends with developers, security experts, and policy makers to study how people introduce anti-security into systems. The recommended guidelines from a complete literature, interviews, and surveys can be used to enhance the quality of the CCAF framework, a live framework that connects to the people, universities and industry. CCAF can be used to develop a process model for software security and demonstrate it as an architectural framework for software security improvement. Finally, CCAF can collect best practice guidelines for software security and build an automated software system.

The importance of building cyber security and trustworthy system in today's internet based applications such as e-commerce, banking, financial sectors, social networking, and others. Hence developing a model for building-in security and assessment framework helps people and users alike to develop interdisciplinary collaboration involved with resiliency of social networks and social behaviors. We can also a build-in direct link to helpline and social services. The research will involve multidisciplinary research on building a theoretical framework for building security, people's concerns, and trust. Also will involve analyzing and collecting best practices and model the expert knowledge to build a software system which can automatically assess and identify cyber security, flaws and untrustworthiness.

3.2. Component services for resiliency

Software component services for resiliency are presented in section with detailed aims and objectives to deliver the required methodology.

A. Aims and Objectives

To ensure the methodology can work well, all software components in the proposed framework, Cloud Computing Adoption Framework (CCAF), should include the build-in resiliency, safety, and security of software systems, of software systems, with the following aims:

- CCAF can provide software resiliency and social engineering for software security;
- CCAF can allow users to assess and improve organizational security using a capability improvement model which will be produced as one of the outcomes of this project and
- Automated CCAF software system is used to build secured software systems and autonomic knowledge based best practice guidelines.

CCAF has five component parts consisting of resilient software systems development model, best practice guidelines, social engineering for software security, requirements engineering for software security, and building an automated system for improvement. All the models, methods, process, and tools will be evaluated with companies and organizations (Merkow and Raghavan, 2010; Rehman et al., 2013).

B. Resilient Software Systems Development Model

This component exists in the CCAF to develop a resilient and secured system for implementing a build-in systematic approach. CCAF illustrates the principal of the resilient software system and its characteristics for building such a system from the start of the software lifecycle implementing and improving based on McGraw's (2006) and Ramachandran's (2012) work. Our new contribution is to enforce the build-in software security concepts on top of the systematic approach to connect to the current practices. This has become more important for emerging applications such as cloud computing where reuse and resources and computing powers have been shared.

C. Best practice guidelines

This component exists in the CCAF to develop a set of best practice guidelines on building-in resiliency and software security. CCAF is used to demonstrate a complete lifecycle from requirements, design, implementation, and to testing for the development of secured software systems.

D. Social engineering for software security Model

This component exists in the CCAF to demonstrate techniques and methods for social engineering in software security. Current techniques have only been considered for network and internet security but not have been developed for the development of application software systems.

E. Requirements engineering for software security

This component exists in the CCAF to develop a framework for capturing requirements for software security and resiliency to develop an architectural framework for enterprises' services and best practices as in Figure 5 in Section 5.

F. Knowledge Based System for Software Security

This component exists in the CCAF to analyze software systems automatically for software security based on the previous research outcomes from all the CCAF components detailed above. Some examples include the best practice guidelines and software development for various software technologies such as Java and C#.

To this end, we have developed a large scale survey to validate the CCAF framework, components, resilient design characteristics from various vendors. The results show very encouraging study to improve CCAF and have potential to emerge as a de facto standard for resilient systems.

4. SURVEY RESULTS AND ANALYSIS

Conducting a large scale survey and explaining its results for showing how they can be used for the framework development is the first step of the research methodology, which details are going to be revealed in this section accordingly.

Although the UK HM Government (2015) has released their survey results on cyber security, the report does not show any information about the resilient security framework. The responded numbers can vary between questions and questions and there is a lack of consistency in the use of the responded numbers. All questions should remain consistent so that statistical data analysis can be performed. Hence, large scale surveys have been

conducted in the UK in Year 2014 and 2015. More than 2,050 questionnaires were sent to all kinds of IT professionals and academics who have more than 5 years of experience to collect their feedback on security and privacy requirements. Out of 2,050 surveys, 400 valid samples were collected and used of analysis, with 19.5% response rate. Amongst 400 valid respondents, 305 are male and 95 are female. Among these 400 sample sizes, 20% are based in London, 20% are based in the South England, 20% are based in the West and South Yorkshire, 20% are based in the entire Scotland and 20% are from the rest of the UK, thus, this makes a fairly equal distribution. All these results and additional comments are useful for the development of CCAF resilient framework as follows.

Figure 2 shows the results when respondents were asked which aspect of security is seen the most important. Privacy has 150 respondents to support and is the highest amongst all the choices, followed by identity management with 63 respondents, trust with 55 respondents, encryption with 40 respondents, access control with 35 respondents and other type of security solutions with 57 respondents. All forms of biometrics and personal identity management are considered under identity management. Even so, privacy is regarded as the most important and concerned aspect of security. Some respondents have replied that they always have concerns on their privacy settings in the internet and mobile phone services, as well as whether any sensitive data or information can be leaked or spied without their permission.

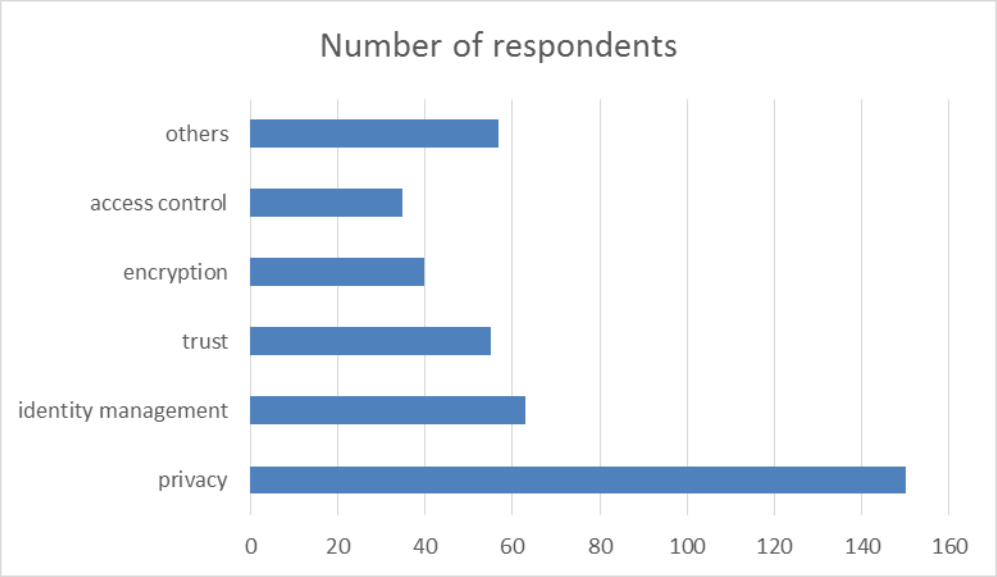

Figure 2: Which aspects of security are seen the most important amongst 400 valid respondents

The next question is whether respondents feel confident and secure with their current security solutions. Unexpectedly 82% do not feel confident. Thus, this leads to the next question about the single solution versus an integrated solution. The aim is to find out whether respondents are confident about their current security solutions which are based on a single solution, either one of the main solutions presented in Figure 2 rather than the combination of a few solutions together. Similar results are presented in Figure 3, which shows 80% feel the integration of multiple solutions is better than the single solution that they have. Supported by Takabi et al. (2010), the adoption of integrated multiple security solution can provide a better and more secure service than the use of a single solution.

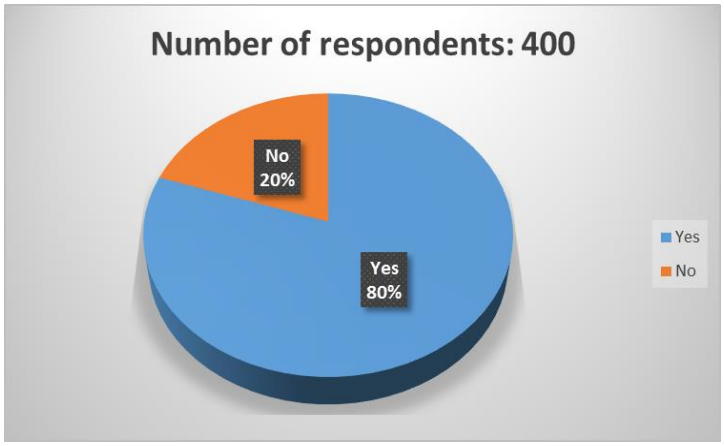

Figure 3: The percentage of respondents feel the integration of multiple solutions is better than the single solution that they have

The next question is whether the respondents have experienced any security breaches they have suffered the most between Year 2010 and 2015. Figure 4 shows the results, whereby the infection by viruses and malicious files is the highest, since 164 respondents have chosen it. It shows infection by viruses, trojans and phishing websites can be seen as the most frequent security breach and security services should always keep their signature and anti-viruses defense up-to-date. The second highest is the theft or fraud including identify fraud, theft by digital means and credit card details reported by 85 respondents. This is a serious offence since each year estimated £27 billion of loss and costs have been estimated (UK Government, 2011). The third highest is the incidents caused by others, which include the infection of viruses and trojans which have taken unauthorized access, leakage of confidential information, breach of data protection laws, unauthorized access to system and data by the insiders reported by 55 respondents. This has been increasingly important due to the rapid growth of data and the need to provide sufficient training to the employees. The fourth highest incident is the data loss, ownership, manipulation and unauthorized use involved with other collaborators, users, clients, former employees and competitors reported by 31 respondents. This is more complicated to handle since it involves dealing with laws, business and complex work relationship. Attacks and hacking by unauthorized use is ranked the fifth reported by 29 respondents since the majority of organizations have done well in the real-time protection of data. However, some organizations have reported that unauthorized access and denial of services have been detected on regular basis and their security solutions have always been kept up-to-date to enforce security. Unexpectedly 36 respondents have reported they do not experience any major security breaches.

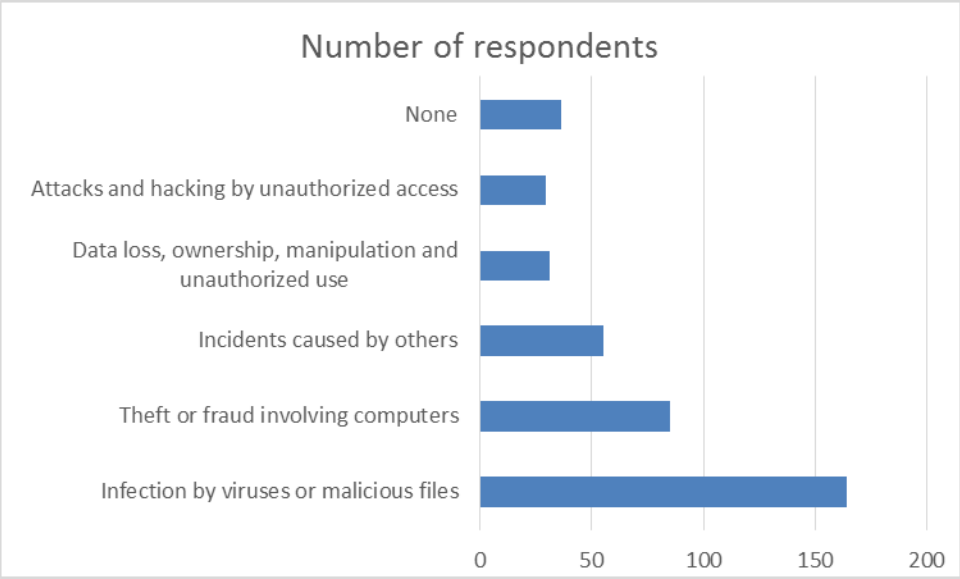

Figure 4: Types of security breaches they have suffered the most between Year 2010 and 2015

All these results suggest that the threats are from viruses and malicious files and identify theft or fraud. While acknowledging the fact that the integration of multiple solutions may provide a greater level of security and protection than the adoption of a single solution, very few literatures have suggested that the integration of different security solution is possible. This leads authors to develop an integrated security framework that blends different types of security techniques and measures together to offer a more robust and resilient security service. From this large scale survey, we have learned an integrated approach to developing resiliency is extremely important for an enterprise cloud solution. In addition the respondents have clearly expressed security of data and disaster recovery are the key to moving to a cloud. Therefore, we have developed our framework taking all this into consideration. In addition, we have adopted CCAF into a group of key impact case studies such as financial cloud, Amazon Web Services, and Emerging Software as a Service and Analytics (ESaaSA) as shown in Figure 5.

5. THE INTEGRATED CLOUD COMPUTING ADOPTION FRAMEWORK (CCAF) FOR SOFTWARE RESILIENCE

The second step of the proposed research methodology is to build a system that can assess and improve cyber security and trustworthy of existing and new systems alike by using the large scale survey results as input. Accordingly, this section will base on the survey results shown in Section 4 to propose an integrated Cloud Computing Adoption Framework (CCAF), and next section will then explain how CCAF framework can be used as a business resilient framework to provide the competitive edge.

Section 3.2 presents software components with five major types of desirable aims and characteristics. High quality software requires fulfilling all these criteria. Similarly, all different components should be blended together successfully as an integrated framework to ensure that the maximum level of efficiency can be achieved. As discussed in Section 4 about reflecting the collective user requirements from the large scale surveys, the system design of an integrated security solution may offer a better security and protection than the adoption of a single security solution to combat the threats from the viruses, trojans and identify theft or fraud. Hence, all these requirements have become the inputs to develop an integrated security framework which can provide resilience and robustness to withstand different types of malicious files, digital theft, unauthorized access and attacks. In order to demonstrate the integration can be delivered, the integrated Cloud Computing Adoption Framework (CCAF) is presented in Figure 5. Surrounding the CCAF, there are three complementary blocks interact with each other to form a complete framework. The framework starts from a Multi-Layered Cloud Security consideration to build a cloud service by according to the Cloud Computing Adoption Framework. Subsequently, the framework then uses automated business process to drive the security testing on the built cloud service while measuring its status. Finally, impact case can be implemented by the CCAF is shown at top of the Figure 5. The relationships of the surrounding blocks and the CCAF are organized in following paragraphs.

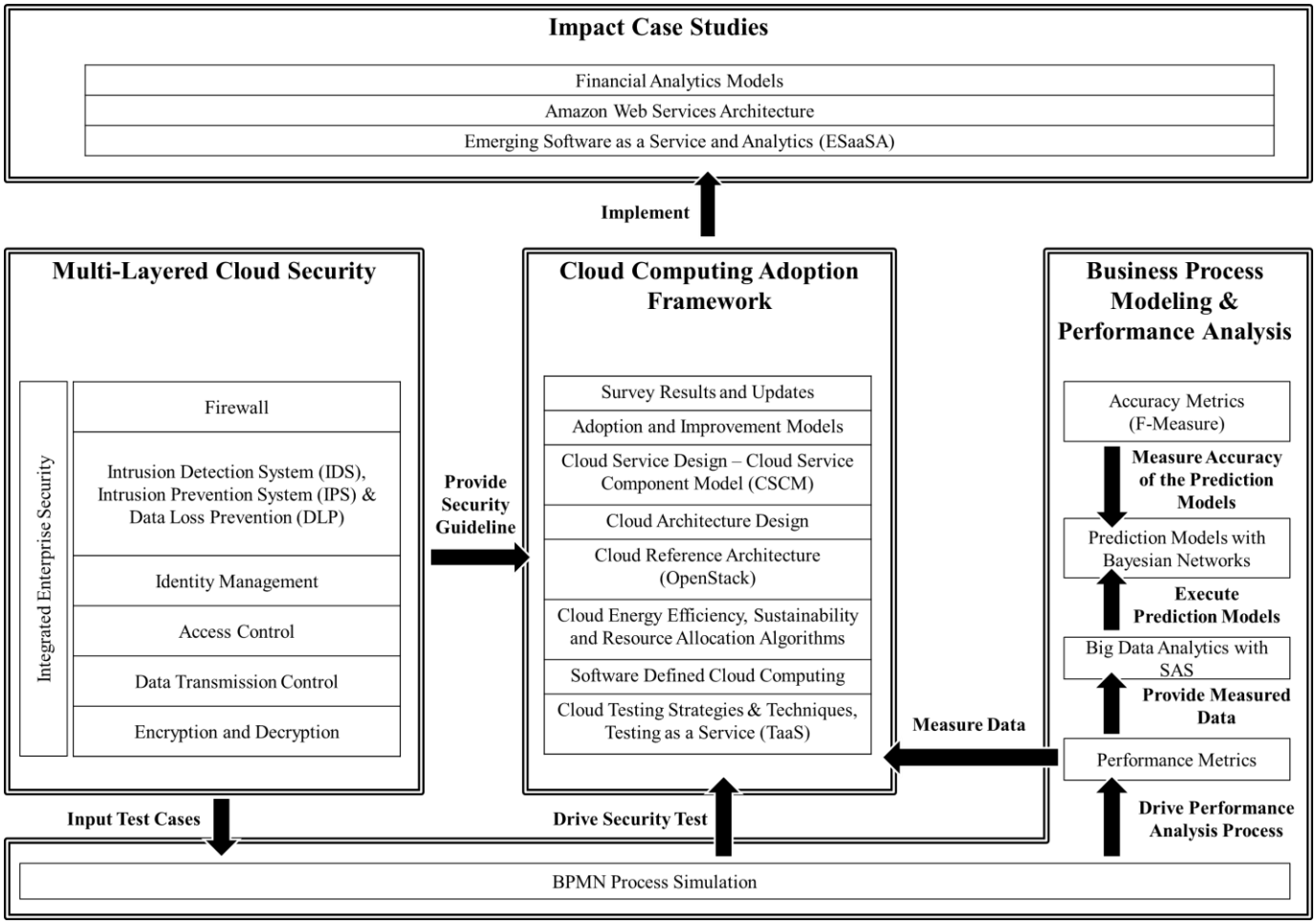

Figure 5: The proposed integrated CCAF Framework

There are four major categorizations of the software components and services with top-down and left-right bilateral approaches. The center of the CCAF framework contains the followings in a top-down approach by starting from requirements: Survey Results and Updates; Adoption and Improvement Models; Cloud Service Design - Cloud Service Component Model (CSCM); Cloud Architecture Design; Cloud Reference Architecture (OpenStack); Cloud Energy Efficiency, Sustainability and Resource Allocation Algorithms; Software Defined Cloud Computing; Cloud Testing Strategies & Techniques, Testing as a Service (TaaS). All of these are the core and essential parts of the framework. From the top to bottom approach, survey results and updates are important to the development of CCAF framework since all the requirements from active users and the stakeholders should be collected and fully translated to the project development of the CCAF framework. The detailed survey questions have been conducted for the following reasons. First, surveys can collect the user requirements and ensure that CCAF can meet those requirements and avoid any pitfalls recommended by a large number of respondents. Second, any security and privacy concerns can be updated in the latest CCAF development. Following that, the improvements models are based on the user requirements and the reflection of the software services. It then requires a robust system design to ensure requirements can be fully translated to software development. In the architecture design, agile methods and software engineering will be implemented together with reference architecture such as OpenStack to maximize the impact. Useful algorithms are then developed to ensure security, functionality and usability to be well balanced, which can be further assisted by software defined Cloud Computing approach as demonstrated by Chang (2014, 2015 a) and Chang et al. (2015). Cloud Testing strategies, techniques and Testing as a Service (TaaS) can be fully implemented to ensure that all services can pass vigorous tests, checks and validation. All these can improve the security of the software components and services. Results from

experiments and simulations can support the validity of the framework (Merkow and Raghavan, 2010; Rehman et al., 2013; Rozanski and Woods, 2011).

On the left of Figure 5, it is the Multi-Layered Cloud Security adapted to all software services and components especially to the CCAF. It provides CCAF with a comprehensive security guideline for developing a cloud service. The Multi-Layered Cloud Security contains the followings in the top-down sequence by starting from the external network defensive component: Firewall; Intrusion Detection System (IDS), Intrusion Prevention System (IPS) & Data Loss Prevention (DLP); Identity Management; Access Control; Data Transition Control; and Encryption and Decryption. In addition to the multi-layered structure, an Integrated Enterprise Security also stands aside layers to ensure end-to-end security. Firewall acts on the first layer of defense for all types of incoming and outgoing messages. The next layer is IDS, IPS and DLP since they need to identify all the malicious files and prevent them in the first instance. In case they are getting into this layer, they will be moved to the quarantine area for further action. The next level is identity management to ensure that the right person can get the right level of access. Following this, access control is used to ensure that the right person had the right level of permission and access to directories and files that he or she has. Data transition control is in place to ensure that the type of data a user asks is what he or she needs and can access to. Encryption and Decryption are then in the next layer of defense since it ensures that no malicious files can pretend to be the right one to affect users' accessibility and then he or she may carry them to the places where damage will happen. All these components and services are integrated by the Integrated Enterprise Security and seamless to the users during the service to ensure end-to-end security.

On the right of Figure 5, it is Business Process Modeling & Performance Analysis. It contains the followings in a process driven sequence: BPMN Process Simulation; Performance Metrics; Big Data Analytics with SAS; Prediction Models with Bayesian Networks and Accuracy Metrics (F-Measure). BPMN simulations are useful to understand how long and what sorts of actions will be required at the period of emergency. For example, if the data center has been hacked and compromised, how long will be required to take full control and what sorts of data have been compromised can be simulated by the BPMN (Chang and Ramachandran, 2016). Results can return the stakeholders. Thus, collecting performance metrics are important to allow all the stakeholders understand the situations with empirical evidences. In order to simplify the complexity to understand, Big Data Analytics is required so that all the complex data can be simulated within seconds, and the use of SAS solutions can help achieve this. Before deriving any conclusion, Prediction Models with Bayesian Networks are useful since the stakeholders can identify the forecasted outcomes and actions for the following micro-steps before taking a full control of security breach or severe service downtime caused by fire, flood or blackout. By collecting the actual and predicted results and make direct comparisons, F-measure can help the stakeholders understand the accuracy of their predictions and thus can revise their inputs, models and expectations in the subsequent predictions and actual result analysis (Chang and Ramachandran, 2016; Ramachandran et al., 2015).

Impact case studies are essential to the CCAF since a valid and live framework should offer users the list of recommendations and details about how organizations can successfully follow steps and guidelines recommended by the framework. If a framework does not provide full details and cannot explain how they can be adopted partially or fully by organizations or groups of individuals, then it is less convincing and relevant to those who are in need of improving their situations and providing impacts to their business and technical needs such as providing better software as a service and quality of service, connecting all the users and stakeholders at the ease and enforcing data and service security at all times (Chang, 2015 a). It can start with Financial Analytics Models to calculate the risks involved with the associated expected and actual return, which can be in profitability, improvement in efficiency and user satisfaction depending on different business goals. For example, profitability is the chosen focus. All the status of risk and return can be tracked and monitored in real time. While some or most of services are delivered by private clouds due to the better management of services and security, the testbeds or volatile services can use Amazon Web Services (AWS) as the testbed to demonstrate a successful proofs-of-concept first before deploying in the private clouds for production and service delivery. Emerging Software as a Service and Analytics (ESaaSA) can be used for two reasons. First, the ESaaSA can present complex data into a way that the stakeholders can understand through the intelligent algorithms, visualization and analytics. Particularly in visualization and analytics, all the business analysts have been trained and accustomed to the use of them to provide them the edge and readiness over their competitors. ESaaSA can also blend public and private clouds

together without implementing large scale hybrid clouds since data can be shared and jointly used to analyze results and interpret them in a way that businesses can fully utilize.

The integrated CCAF security framework can work with different aspects of security requirements and emphasis together. By blending the core activities in four major services under "Multi-Layered Cloud Security, "Cloud Computing Adoption Framework", "Business Process Modeling and Performance Analysis" and finally "Impact Case Studies", the integrated security solution can provide a more holistic approach and comprehensive method in dealing with enterprise security. All services can be kept update-to-date and work collaboratively with other streams of services to produce a greater impacts. Hence, the integrated CCAF security framework is aimed to be an emerging service and analytics for security, since all abnormal activities can be detected and alarmed in real time, as well as the improvement in the quality of services and the confidence in providing enhanced services than the adoption of a single solution. All the security features can safeguard all the services and data under the protection of the integrated CCAF framework.

6. BUSINESS RESILIENCY FRAMEWORK

As the second half of the second step of proposed research methodology, this section explains how our proposed CCAF framework as shown in Section 5 is also a business resiliency framework. Pettit et al (2010) demonstrate resiliency for supply chain business and explain its significance to business operations. They use resiliency framework to minimize risk and ensure business can move forward. Business resiliency can be used as an integrated approach as follows. The overall framework of the mission and business level resiliency, as shown in Figure 6 is directly related to the continual optimization of a utility derived from the services being performed within the infrastructure. The simplest form of this *utility* has three primary components:

- **Value of the service being successfully rendered:** The service could be either directly or indirectly involved in the value creation of the mission or business. The value created is often dependent on the service quality (measured in terms of Key Performance Indicators or KPIs)
- **Cost of resource:** Multiple methods need to be executed in order to deliver the service. Each of these methods will need multiple compute, storage, network, software, and application resources, and hence incur cost.
- **Cost of failure:** There is also cost associated with the failed delivery of the services (including the lack of availability of these services or the services were not delivered according to schedule).

This utility is the value created by the delivery of service, subtracting the cost for delivering the service and the cost associated with a potential failure, which is weighted by the probability of such a failure. This business resilient framework allows us to properly calibrate the value at risk for any given service, so that eventually the overall metric will be risk adjusted cost performance (i.e. risk adjusted cost vs. risk adjusted performance).

The business resilient framework is aimed to align business with operational activities, since recommendations and best practice approaches can be implemented with any projects and initiatives. All the business performance key indicators (PKI) can be identified, measured and evaluated. The expected goals can be set and measured over a period of time. The actual outcomes have been recorded and compared with the expected targets. If the actual outcomes are better, businesses can adopt lesson learned and adapt them into similar projects and cases to replicate success. If better outcomes are expected, businesses need to identify where goes wrong, list the areas of improvements, set targets and evaluate whether improvement has been made over a period of time. While all these data have been collected, appropriate quantitative analysis is required to understand how well businesses have performed, such as their new or existing Cloud Computing projects. A recommended model is the use of Organizational Sustainability Modeling (OSM) which measures the expected and actual outcomes and compares them directly through computational analysis (Chang et al., 2015). OSM outputs show a list of PKIs to inform the stakeholders how well their new or existing services have performed and identified areas of the strengths and weaknesses of their new or existing Cloud Computing services. Outputs in visualization allow the stakeholders to understand the underlying complex concepts within seconds so it provides businesses the

competitive edge as demonstrated by supporting OSM case studies. The use of CCAF framework is in complimentary of the adoption of OSM analysis, since the integrated approach can collect a variety type of business data for different departments, so that all the analysis can be evaluated and reported back to the management. Therefore, businesses can align different departments more proactively, check progress up-to-date, forecast problems ahead and devise any solutions to resolve ongoing or new issues.

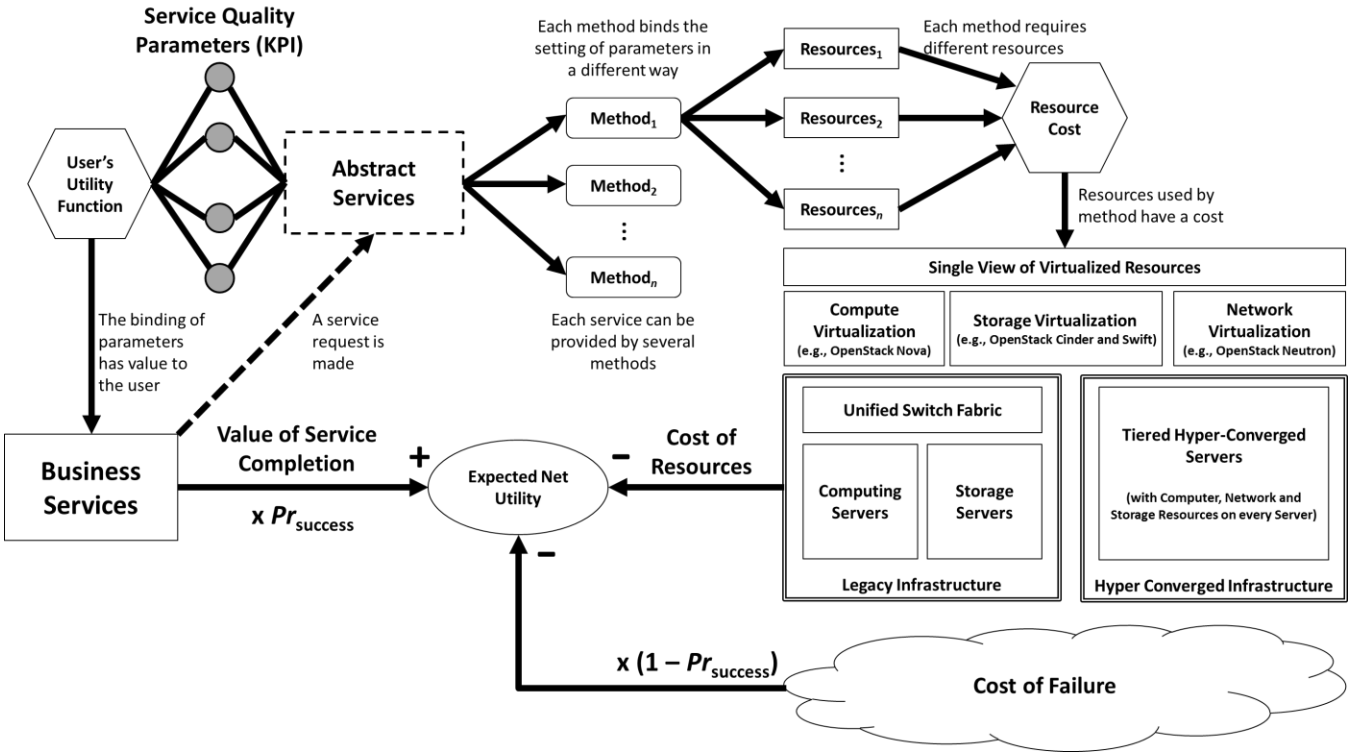

Figure 6: Resilient computing selects the method which maximizes expected net utility for a given service (a.k.a. value@risk)

7. CHECKING THE COLLECTIVE REQUIREMENTS WITH CCAF

In the last step of the proposed research methodology, it will evaluate user evaluation and metrics on cyber security and trustworthiness of systems to justify the collective user requirements (see Section 4) for the CCAF development (see Sections 5 and 6) with rationale explained for summary of comments given by the respondents.

It is important to double check with the collective user requirement as the saying of "wisdom of the crowd" can be used for the CCAF development, particularly checking the effectiveness of the technical integration and alignment with business operations introduced in Sections 5 and 6. Questionnaires together with the brief explanations on CCAF architecture and integrated security features have were sent to the 400 respondents described in Section 4. Only 220 replied with a good 55.0% response rate. Additional comments were recorded. The first question is to provide ratings based on the system design, functional specifications and proposal for the CCAF. Each respondent has been asked to provide a rating between 1 and 5, whereby 1 is the lowest and 5 is the highest rating to evaluate whether CCAF is a useful framework with the option to write down additional feedback. All the scores have been recorded and analyzed. With regard to our own benchmark, it is similar to the UK National Student Survey (HEFCE, 2015) which has been conducted over 30 years of track record and the same principle can be applied for quality assurance (Qin et al., 2003; Richardson et al., 2007). In the benchmark we use, a score of 3 does not mean the respondent is satisfied with the work or service they have received. In other words, a score between 1 and 3 are considered not satisfied. Only scores with 4 and 5 out of 5 are considered satisfactory.

Figure 7 shows the percentage of the respondents' opinions on the CCAF. A majority of 69% has provided scores of 4 and 5 and agrees that it is a sound good framework. On the other hand, 31% of respondents has provided scores between 1 and 3 and disagrees. With regard to the data analysis of all the collected scores, ***the mean value is 3.49, with standard deviations of 0.568 with p-values less than 0.05***. These results show there is a good consistency between all the collected results and rooms for further improvement to aim for the mean score of 4.0. While asking respondents' feedback, those who have voted satisfied think that CCAF is a relevant architecture and has the considerations of blending different aspects together to offer an integrated approach. CCAF framework provides its strength on enterprise security and business alignment. Those who have voted dissatisfied pointed out that there is a lack of simulations and experiments to prove the validity and robustness of the framework. Much more experiments should be designed and conducted to ensure that the proposed framework is resilient towards the unauthorized access and attacks from viruses, trojans and identity thefts.

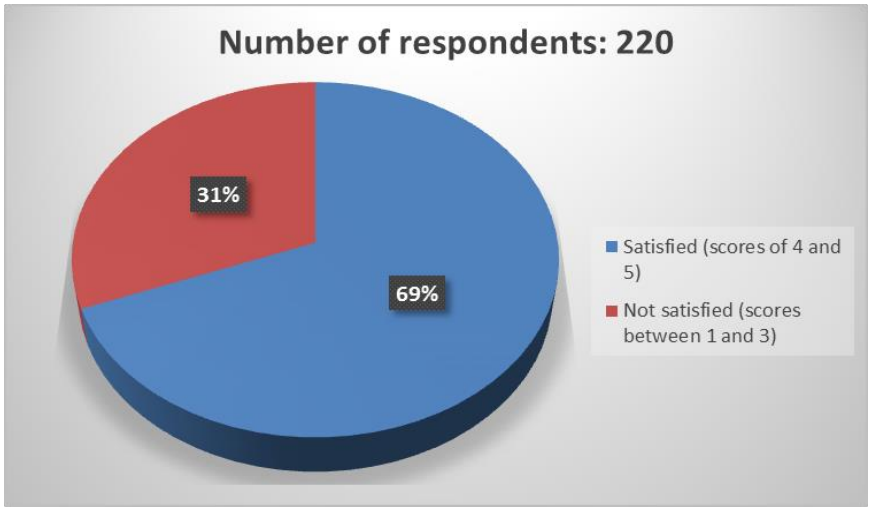

Figure 7: The percentage of respondents' opinions on the CCAF

The second question is more open ended, asking what respondents will like to see what sort of tests or features in CCAF. Shorter questions can guarantee a higher response rate in this case. The second major question can play important role to receive constructive feedback on what the user community would expect from a CCAF security framework. In other words, all respondents can provide their comments regardless of their feedback in question 1. Their comments have been recorded and summarized in Figure 8. The highest feature to have is "tests with viruses, trojans and malicious files with 102 nominations. The main reason is that all security solution should undergo the real tests with those malicious files and have tests to validate the resilience of the CCAF framework. The second highest feature is the "multi-layered security with integration with other services" with 39 nominations. The main reason is more supporting cases that CCAF can work with other types of security solutions are required. The third highest feature is ethical hacking with 32 nominations since a large scale penetration testing is required to ensure that the CCAF framework can withstand all types of ethical hacking. The fourth highest feature is NoSQL tests with 11 nominations, since a lot of hacking has happened on SQL injection and vulnerabilities on databases. Hence, the use of NoSQL databases are less likely to happen since SQL injection will not work on NoSQL databases. There are 6 nominations commenting that other types of empirical tests should be required since those tests will be useful for resilience. Six respondents have no comments on the CCAF development.

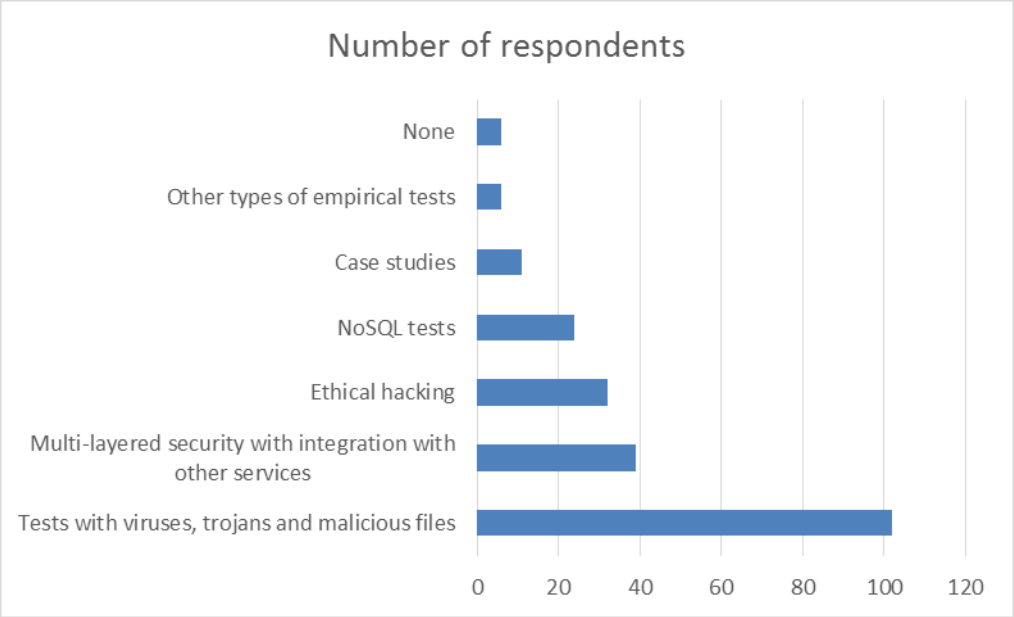

Figure 8: Summary of the respondents' comments

Based on all these feedback, the CCAF security framework will require integrating other technologies such as OpenStack based solution since OpenStack is an open platform for Cloud Computing. CCAF framework should explain how the multi-layered protection can work and adopt ethical hacking. Large scale penetration testing and ethical hacking, such as the injection of the known viruses and trojans in past years, are required to test the robustness of the framework. Continuous attacks on identity management and NoSQL tests should also be given to test whether the proposed solution can withstand different types of attacks. Some outputs can be presented in the form of visualization and analytics, so that the stakeholders and users without much technical background can understand the interpretations and analysis from the intelligent CCAF service. If a proposed CCAF framework can demonstrate all these desirable outcomes, it is moving towards working and demonstrating as an emerging service and analytics for Cloud Computing.

The third major question is to ask how much money the respondents' organizations will spend on security and privacy in the next year (2016) and next three years (2016-2018) in British pounds and write down which aspects of security they will invest. The aim is to give the stakeholders of all types an overview and rationale about the future spending on security and privacy. 10 respondents have answered "don't know" and thus only 210 valid sample size has been used for analysis. All the spending ranges are listed down at the bottom of Figure 9. Out of 210 valid respondents, the spending on security and privacy for 2016 is less than three-year spending in general. For Year 2016 spending, the number of respondents for all the spending ranges is 24, 37, 59, 41, 13, 10, 6, 17, 3, 0 and 0 respectively. The most number of respondents have indicated the annual spending will be between £30,000 and £50,000. For Year 2016 to Year 2018 spending, the number of respondents for all the spending ranges is 10, 26, 42, 34, 29, 15, 11, 22, 16, 4 and 2 respectively. Although the annual spending will be between £30,000 and £50,000 is still the highest for Year 2016 and Year 2018, the spending is well distributed in all different ranges. Additionally, there are more than 44 individuals' organizations will spend more than £1 million compared to 20 of them for Year 2016 spending alone. All the results show that there is an increased acknowledgement and awareness for security and privacy investment. Similarly, the challenges related to cyber and data security have been increasingly important for organizations based in the UK.

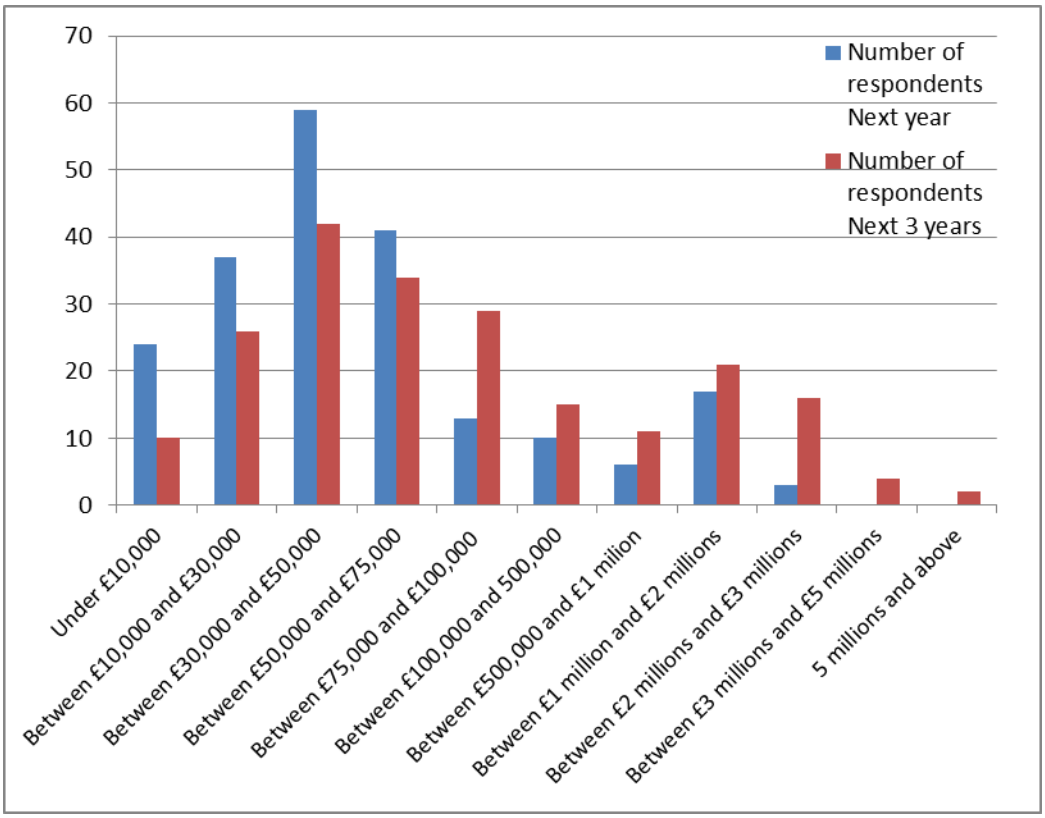

Figure 9: The future spending on security and privacy in the next year (2016) and next three years (2016-2018)

Respondents have also been asked to choose the area that will have the highest amount of spending if they know, with multiple choices given to them, including new systems and hardware, new software, upgrade on existing hardware, upgrade on existing software, consultancy, staff training and others. Each respondent can only choose one and if he/she chooses others, then provide more information. Results are shown in Figure 10. The highest percentage is new software purchase (21%), followed by consultancy (20%), upgrade on existing software (19%) and then staff training (17%). The results show that purchase of new software and upgrade on existing software have played influential roles in security and privacy investment since more robust and better quality of software and software services are required to keep security of data, servers, information and day-to-day activities up-to-date. Consultancy is the second highest due to two reasons based on our results. First, some security challenges are not easy to be resolved and external expertise is brought in to resolute ongoing and new issues associated with upgrade or purchase of new software/services. Second, consultants are used to speed up the completion of internal projects or troubleshoot any issues with clients' software/services. Occasionally consultants provide staff trainings if required. The staff training is the fourth highest since some security software, hardware and services require very sophisticated skills and knowledge to battle with security challenges, including techniques in intrusion and detection, data recovery, anti-hacking, encryption, troubleshooting, certifications and on-job training. Employees at different levels of ICT skills will need to undergo training to ensure their knowledge and skills are up-to-date to prevent themselves become victims of fraud or any forms of security breach.

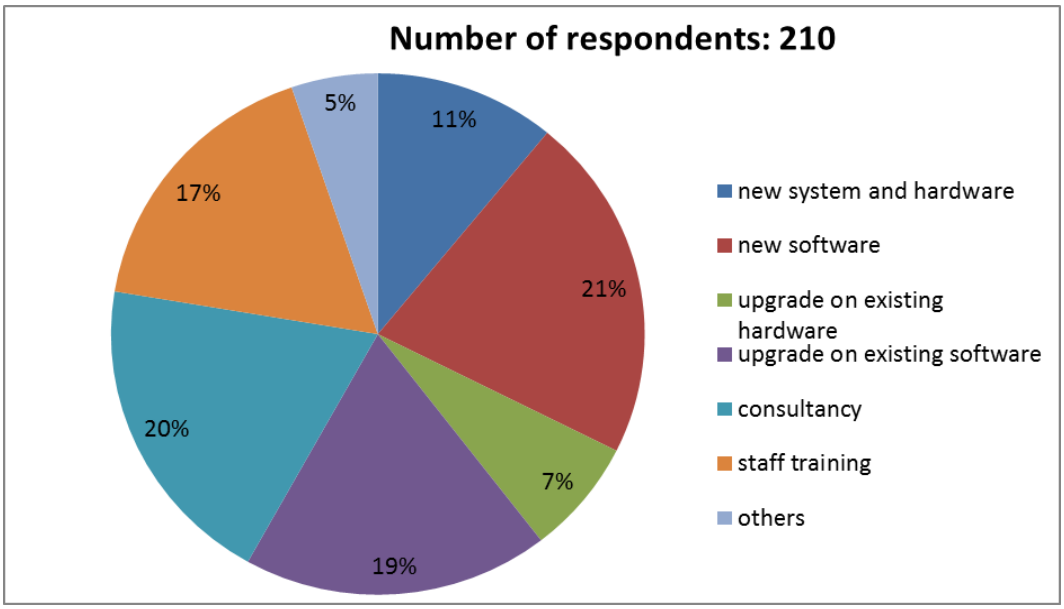

Figure 10: Percentage of distribution on security spending categories

8. DISCUSSION

The topic of discussion is focused on how software resiliency and security improvement can provide added values for enterprise security to ensure CCAF framework provide a real-value emerging service for Cloud Computing. A recommended approach is to blend the all the targets into multi layers of services and ensure that goals in each target can be met before moving to new goals of the following target.

The first target is the Cloud Adoption Model with seven steps to achieve the target. The first step is the initial IT cost assessment, since the organization should understand how much they can spend and afford before, during and after the service delivery or project. The second step is Cloudonomics study to realize the cost effectiveness through the service delivery or project (Weinman, 2012). The third step is migrating application to a Cloud incrementally since the organization should identify problems and challenges involved and whether steps can be reproduced easily for a full migration. The fourth step is the selection of private versus public cloud since organizations should fully be aware all the options available, what they can do for each and whether integration in the future is possible, costs involved and easy to achieve. The fifth step is Cloud user feedback and improvement since users should be involved early and their participation and feedback can offer strong points for service level improvement throughout the software lifecycle. The sixth step is continuous monitoring cost effectiveness and improvements, since if costs are likely to be higher than the expected targets, remedy actions and plans should be in place to confirm a good justification of cost, resource and time involved. If more funding is required, then appropriate actions can be made in the next step, or if any areas that require urgent improvement, they can be the target for the next step, business process model for performance evaluation to fully justify the status in the first target.

The second target is the development and delivery of multi-layered security since a single security recommendation is not enough to provide better security services as illustrated by experiments conducted by survey results in Figure 3. Multi-layered security can enforce the data and service security to ensure that all the data are safe and encrypted as illustrated in Section 5. In the example demonstrated by Chang and Ramachandran (2016), the first layer of security is firewall and access control to ensure that only the right person with authentication and authorization can access. The second layer, identify management, enforces this aspect to ensure each user's identify can be cross checked and remain robust. If any malicious files are found, they can be removed. The third layer is encryption and decryption security, since a small percentage of files can be pretended to be the normal files as conducted by experiments in Chang and Ramachandran (2016). The use of advanced algorithms can

ensure that no other malicious files can be disguised as normal files. Figure 11 shows a CCAF with Resiliency and sustainable cloud. More organizations and users would like to see cloud data centers is capable of withstanding any cyber-attacks, floods, fire, theft, server and network failures, hardware failures, and natural disasters without losing its services nor more importantly its data. Hence, each data center should have a mirror data center with secured data and services in case of any disasters, or adopt some intelligent services that can recover the lost data efficiently and effectively in an acceptable time frame (Chang, 2015 b).

The third target is Big Data analytics. As discussed in Section 7, all the complex data should be analyzed and then presented in a way that those without prior knowledge can understand. This can provide the edge of competitiveness for business analysts since more time can be spent on understanding the consequences and followed up actions of these analyses. Big Data Analytics can also present work from one discipline to another and try to find any correlation in between. For example, the links between Cloud Computing and financial modeling can be achieved by jointly delivering Business Intelligence as a Service to compute the status of risk and return in real time (Chang, 2014). Cloud Computing and bioinformatics services can provide Healthcare as a Service for medical staff and scientists. The use of analytics and visualization can present biological science investigations such as the growth of tumor, the protein and immunity studies (Chang, 2013). This can bridge the gap across different disciplines.

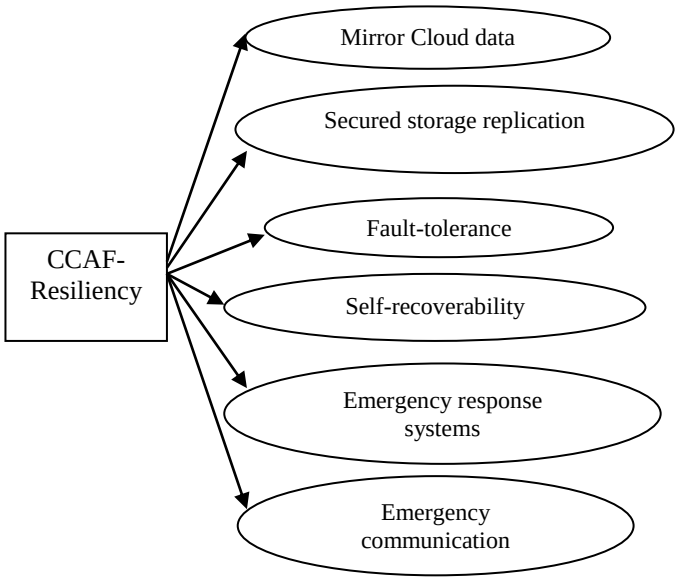

Figure 11: CCAF Resiliency and sustainable cloud

The fourth target is the demonstration of experiments and tests to show that CCAF can withstand a large scale attacks from SQL injection, viruses and trojans of the previous years, malicious files and other known attacks under the ethical hacking environment. Results will need to demonstrate the resilience and robustness of the CCAF framework to show that it is a truly emerging service to provide safety and protection to all data and services involved. The easy-to-use features will be provided to show that outputs can be interpreted without much effort by the use of analytics and visualization.

The fifth target is to make CCAF a business resilient framework to allow businesses to align their departments and operations more closely and proactively. The use of CCAF framework can identify PKIs' measures and evaluates the data between expected and actual outcomes of their new and existing Cloud Computing projects as the Utility introduced in Section 6. The stakeholders can use CCAF framework to provide the competitive edge since problems can be reported and analyzed and the management knows where are the areas of improvement, progress up-to-date and any rising issues to resolve. While taking all factors and targets into considerations, the sub-model presented in Figure 11 of the CCAF is one of the unique contribution to resiliency and sustainability of cloud computing and its technologies.

9. CONCLUSION AND FUTURE WORK

Enterprise Cloud Computing is increasingly important and the approach is to introduce software resiliency whereby success factors and components in each service have been presented. The focus in this paper is to present a framework to enforce and deliver enterprise security. CCAF is the architectural framework that can provide detailed guidelines for software component and resiliency and explain the relationship between each component and each major service. All different requirements can be seamlessly joint up together to provide a greater impact with real case studies in place. The details in each layer, each function and how they can be blended together to achieve goals and plans for enterprise security have been explained. Surveys have been taken with 400 valid respondents and their feedback has been very useful for the development of the CCAF framework. All the user requirements have been essential to build the resilient framework. Four topics have been discussed to show that CCAF framework can be an emerging service for Cloud Computing that provide real protection from hacking, unauthorized access and attacks with analytics services to explain interpretations of security service. All survey results acknowledge that the rising significance of security and privacy spending and more organizations have invested more in the following three years to ensure they can provide better protections to their employees and clients, better security solutions in place and get themselves ready for the emerging services for security.

Future work will include the integration with more services such as Education as a Service, Financial Prediction and Quality as a Service and Security as a Service to explain how different service component can work together to achieve software resiliency and offer real case studies to provide greater impacts to research communities. Vigorous tests will be conducted to illustrate software resiliency. Experiments and simulations will be undertaken and empirical investigations will be demonstrated to support the validity and robustness of the CCAF framework. Being a business resilient framework, CCAF framework can measure KPIs, analyse the performance of Cloud Computing services and provide businesses critical values for agility, efficiency and alignments with operational activities. The adoption of CCAF framework provides a real and useful emerging service for Cloud Computing.

Acknowledgment

Part of this study is conducted under the “Big Data Technologies and Applications Project (1/4)” of the Institute for Information Industry which is subsidized by the Ministry of Economic Affairs of the Republic of China. This research study has been led, designed and evaluated by Dr. Victor Chang with his private resources in England.

References

Chang, V. (2013). Cloud Bioinformatics in a private cloud deployment. Advancing Medical Practice through Technology: Applications for Healthcare Delivery, Management, and Quality: Applications for Healthcare Delivery, Management, and Quality, 205.

Chang, V. (2014), The Business Intelligence As a Service in the Cloud. Future Generation Computer Systems, 37, 512-534.

Chang, V. (2015 a). A proposed Cloud Computing Business Framework. ISBN: 9781634820172 (print), Nova Science Publisher.

Chang, V. (2015 b) Towards a Big Data System Disaster Recovery in a Private Cloud. Ad Hoc Networks, in press.

Chang, V., Walters, R. J., & Wills, G. (2015). Organisational sustainability modelling—An emerging service and analytics model for evaluating Cloud Computing adoption with two case studies. International Journal of Information Management, in press.

Chang, V., Ramachandran, M. (2016) Towards achieving Cloud Data Security with Cloud Computing Adoption Framework, IEEE Transactions on Services Computing, forthcoming.

Curphey, M., & Arawo, R. (2006). Web application security assessment tools. Security & Privacy, IEEE, 4(4), 32-41.

Friedman, A. A., & West, D. M. (2010). Privacy and security in cloud computing. Center for Technology Innovation at Brookings.

Gabrys, E. (2011). Encyclopedia of Information Assurance, Taylor Francis Online.

Gillies, A. (2011). Software quality: theory and management. Third edition, publsihed by Lulu. com.

HEFCE (2015), National Student Survey Results, accessible on http://www.hefce.ac.uk/lt/nss/results/2015/, accessed on 29 September 2015.

Holling, C. S. (1996). Engineering resilience versus ecological resilience. Engineering within ecological constraints, 31-44.

Li, C. S, (2014). Resilient Computing, technical report, IBM.

McGraw, G. (2006). Software security: building security in (Vol. 1). Addison-Wesley Professional.
Curphey, M., & Arawo, R. (2006). Web application security assessment tools. Security & Privacy, IEEE, 4(4), 32-41.

Merkow, M. S., Raghavan, L. (2010) Secure and Resilient Software Development. CRC Press.

Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: development of a conceptual framework. Journal of Business Logistics, 31(1), 1-21.

Qin, S. J., & Badgwell, T. A. (2003). A survey of industrial model predictive control technology. Control engineering practice, 11(7), 733-764.

Rajkumar, R. R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. In ACM Proceedings of the 47th Design Automation Conference (pp. 731-736).

Ramachandran, M. (2008), Software components: best practice guidelines and applications, Nova, NY.

Ramachandran, M., de Carvalho, R. A. (Editors, 2010). Handbook of Software Engineering and Productivity Technologies: Implications for Globalisation, Information Science Reference, IGI Publishers, USA, January.

Ramachandran, M., (2012), Software Security Engineering: Design and Applications, Nova Science Publishers, New York, USA. ISBN: 978-1-61470-128-6.

Ramachandran, M., Chang, V., & Li, C. S. (2015). The Improved Cloud Computing Adoption Framework to deliver secure services, In Emerging Software as a Service and Analytics 2015 Workshop (ESaaSA 2015), in conjunction with CLOSER 2015, Lisbon, PT, 20 - 22 May 2015.

Richardson, J. T., Slater, J. B., & Wilson, J. (2007). The national student survey: development, findings and implications. Studies in Higher Education, 32(5), 557-580.

Rozanski, N., Woods E. (2011), Software systems architecture: working with stakeholders using viewpoints and perspectives. Addison-Wesley.

Rehman, S., Shafique, M., Aceituno, P. V., Kriebel, F., Chen, J. J., Henkel J. (2013). Leveraging variable function resilience for selective software reliability on unreliable hardware. In Proceedings of the Conference on Design, Automation and Test in Europe, EDA Consortium, pp. 1759-1764. March.

Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, (6), 24-31.

TRI (2009), Torrens Resilience Institute, technical paper, access on 7 September 2015 http://torrensresilience.org/characteristics-of-resilience.

UK Government (2011), The Cost of Cyber Crime, technical report, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf , accessible on 16 September 2015.

UK Government (2015). 2015 Information Security Breach Survey. Report conducted by PWC. http://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-02.pdf, accessible on 16 September 2015.

Weinman, J. (2012). Cloudonomics: The business value of cloud computing. John Wiley & Sons.