Recommendations and Best Practices for Cloud Enterprise Security

Muthu Ramachandran
School of Computing, Creative Technologies, and Engineering, Leeds Beckett University
Headingley Campus, Leeds LS6 3QS UK
e-mail: M.Ramachandran@leedsbeckett.ac.uk

Victor Chang
School of Computing, Creative Technologies, and Engineering, Leeds Beckett University
Headingley Campus, Leeds LS6 3QS, UK
e-mail: V.I.Chang@leedsbeckett.ac.uk

***Abstract*— Enterprise security is essential to achieve global information security in business and organizations. Enterprise Cloud computing is a new paradigm for that enterprise where businesses need to be secured. Enterprise Cloud computing has established its businesses and software as a service paradigm is increasing its demand for more services. However, this new trend needs to be more systematic with respect to Enterprise Cloud security. Enterprise Cloud security is the key factor in sustaining Enterprise Cloud technology by building-in trust. For example, current challenges that are witnessed today with cyber security and application security flaws are important lessons to be learned. It also has provided best practices that can be adapted. Similarly, as the demand for Enterprise Cloud services increases and so increased importance sought for security and privacy. This paper presents recommendations for enterprise security to analyze and model Enterprise Cloud organizational security of the Enterprise Cloud and its data. In particular, Enterprise Cloud data and Enterprise Cloud storage technologies have become more commonly used in organization that adopt Cloud Computing. Therefore, building trust for Enterprise Cloud users should be the one of the main focuses of Enterprise Cloud computing research.**

Keywords- Cloud enterprise security; Security framework; Cloud security best practice

I. INTRODUCTION

Enterprise Cloud computing technology has emerged to provide a more cost effective solution to businesses and services while making use of inexpensive computing solutions which combines pervasive, internet, and virtualization technologies [1-3]. Enterprise Cloud computing is emerging rapidly and software as a service paradigm is increasing its demand for more services. However, this new trend needs to be more systematic with respect to software engineering and its related processes. For example, while dealing with current challenges faced with cyber security and application security flaws, lessons learned and best practices should be adopted [4]. Similarly, as the demand for Enterprise Cloud services increases and so increased importance sought for security and privacy do. The business of Enterprise Cloud technology can only be financially sustained if we can maintain balance between demand for services in-line with improved Enterprise Cloud security and privacy. Enterprise Cloud computing is also concerned with both service providers and consumers. Enterprise Cloud service providers, including Microsoft, Google, Salesforce.com,, Amazon, Oracle are able to leverage Enterprise Cloud technology with pay-per-use business model with on-demand elasticity by which resources can be expanded or shortened based on service requirements [1, 5]. They often try to co-locate their servers in order to save cost. The every effort by several other enterprises to establish their Enterprise Cloud efforts is used to build their own Enterprise Cloud (private Enterprise Clouds) on their premises. However, it cannot afford to compromise security due to the increasing demands and uses on their applications and data. An important issue is to develop a legitimate and controlled way of establishing service-level-agreements with their clients and to embed these rules to be built-in with services [5, 6]. This offers benefits for consumers, since they can apply best practice security measures, principles, and frameworks [3, 4]. To present our research in the Enterprise Cloud Framework, the breakdown of this paper is as follows. Section II describes the related work for Enterprise Cloud security. Section III presents the issues and opportunities for Cloud Enterprise security. Section IV explains key performance indicators for a good framework and Section V sums up the Conclusion and future work.

II. RELATED WORK

A. Background

In Section II, we present the related work to Enterprise Cloud security, including the background information as follows. Enterprises Engineering incorporates a systematic and comprehensive approach to modeling, designing, and developing enterprises include software and service based enterprises. Chang et al [3] describes a comprehensive framework which can be adopted by enterprises engineering methods and concepts. To further the development, Chang et al [7] demonstrate their framework that uses multi-layered security in Cloud environments. They explain their system design, implementation, experiments, results and their discussion. They also use penetration testing to show their proposed work can filter and block more than 99% of the malicious attack. With an increasing concern for enterprise security, users and organizations can see clearly about the benefits of adopting a security framework [4, 5, 7]

The use of Cloud and internet technology has revolutionized the way we live on a daily basis [4]. The use of internet is growing rapidly from devices, appliances and

Enterprise Cloud computing, which has emerged to address a cost-effective solution for businesses [1, 4]. However, security, trust and privacy are the most common Enterprise Cloud concerns [4-6]. Therefore, achieving security for Enterprise Cloud computing is the main aim of this paper. It is a challenge to protect users from security related attacks which can happen unexpectedly. This is insufficient for Enterprise Cloud service providers who offer three different types of services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Hence, there is a need for going beyond boundaries of existing security techniques such as password protection, virus checks and secured financial transaction techniques. The followings are categories of the broad spectrum of security related research that are undertaken [4, 5, 8]:

- Application software security deals with how we can build enterprises that can automatically protect itself.
- Network (LAN, MAN, GAN), Wireless network security, and Platform Security include Operating Enterprises, Virtualization, and other enterprise software.
- Convergence network security where converging, multi-network media infrastructures, social networks and technologies, which is one of the emerging areas of research.
- Service-oriented security where issues related to enterprise services such as denial of service attacks, distributed denial of services, and web services.
- Enterprise Cloud security deals with services security, data security and privacy so that services delivered and assets are protected.
- Open-source software security deals with issues such as trust, certification and qualification models.
- Software components and architecture security deals with building components and architectures with security can be used as plug-ins.
- Web services security is essential to ensure secure services are delivered with integrity
- Enterprises &Software security engineering deals with building security in (BSI) right from requirements. This also considers developing software applications with BSI.

B. Definitions

In this section, we explain definitions of key security terms used in the Enterprise Cloud security.

Identification is a basic and the first process of establishing and distinguishing amongst person/user. Often we use alphanumerical string as user identification key and some may use your email itself as the user identification key and this can be checked against when a user login into the enterprise. Authentication and authorisation are two distinct forms of allowing users to access what they are not allowed to access any information in the enterprise.

Privacy is the key to maintaining the success of Enterprise 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 & decryption facilities when they need to protect specific information/data/media content.

Integrity is defined as the basic feature of the human being as a process of maintaining consistency of actions, communications, values, methods, measures, principles, expectations, and outcomes. Ethical values are important for Enterprise Cloud service providers to protect integrity of Enterprise Cloud user's data with honesty, truthfulness and accuracy at all time. In Enterprise Cloud computing terms, we can achieve integrity by maintaining regular redundancy checks and digital certification in addition to other basic security features of maintaining identification, authentication, and authorisation. *Durability* is also known as, persistency of user actions and services in use should include sessions and multiple sessions.

In general, we can emphasis on basic of security principle into three main categories as Identification, Authentication, and Authorisation (IAA). The basic process is a cyclic in nature can be defined based on IAA steps. This is a recursive process which must be applied to every action, transactions, and service provisions.

C. Enterprise Security Framework for Enterprise Cloud Services

Capturing and identifying requirements for security explicitly is one of challenges in software engineering. Often security is considered as one the non-functional requirements which have been considered as constraints identified during and after software has been developed and deployed. However, it has an impact on the functionality of the enterprise. Therefore, a priority is to specify security requirements explicitly throughout the security-specific life-cycle phases as part of achieving BSI (security requirements, design for security, security testing & securability testing). Tondel et al. [9] has provided an extensive survey on security requirements methods which help to identify security requirements systematically and structure them. For example, Mead [10] for the SEI's (software Engineering Institute) has identified a method known as SQUARE (Secure Quality Requirements Engineering) and our earlier work on SysSQUARE [8] which has been extended to address Enterprise Cloud security EC-SQUARE (Enterprise Cloud security), is shown in Figure 1, towards enterprises security engineering method. Our extended method consists of nine steps as follow [5, 8]:

- *Agree on security definition* which means to define a set of acronyms, definitions, and domain-specific knowledge needs to be agreed by stakeholders. This will help identify and validate security-specific requirements clearly by stakeholders
- *Identify security goals* which means to clearly define what is expected by the enterprise with respect to security by the business drivers, policies, and procedures

- *Develop security artefacts* which means to develop scenarios, examples, misuse cases, templates for specifications, and forms
- *Perform security risk assessments* which means to conduct risk analysis for all security goals identified, conduct threat analysis
- *Select a security elicitation technique* which includes enterprise identification and analysis of security requirements from stakeholders in the forms of *interviews, business process modelling and simulations, prototypes, discussion and focus groups*. As part of this phase, one has also to identify level of security, cost-benefits analysis, and organisational culture, structure, and style.
- *Elicit security requirements*, which includes activities such as producing security requirements document based security specific principle structure as part of our goal of developing BSI earlier, risk assessment results, and techniques, identifies for analysis such as *business process modelling and simulations, threat modelling, and misuse cases*, etc.
- *Categorise & prioritise security requirements*, which include activities such as classifying and categorising security requirements based on company-specific requirements specification templates and to use our recommended security principles as this will help Enterprises Engineers to apply BSI and track security-specific requirements for validation & verification at all stages of the enterprises engineering life-cycle.
- *Identify enterprises data security requirements*, which include activities on extracting and carefully identifying data security and relevant sub-enterprises such as data centres, servers, Enterprise Cloud VM, and software security, SQL security, and other types of security that are relevant to data. This separation of concerns allows enterprises engineers to integrate, track, design, and develop data security as part of enterprise wide enterprises development.
- *Prioritise security requirements* which include activities of selecting and prioritising security requirements based on business goals as well as cost-benefit analysis.
- *Inspect security requirements* which means to conduct requirements validation process using requirements inspection and review meetings
- *Adopt SDP (Software Defined Protection) Layers for building enterprise security blueprint*

According to our EC-SQUARE model, the first phase starts with identifying security requirements that are achievable and agreed by all stakeholders who are involved in the process. The second step focuses mainly on developing a list all possible security goals as part of the business and functional goals. Thirdly, to develop a list of artefacts that are needed to achieve those security goals. Fourthly, to conduct a detailed risk assessment for each security goal identified and assessed. Clear identification of the requirements of the whole enterprise applications and to extract security requirements for those applications. Interact with stakeholders to clarify security requirements and the technology they want to use, and cost implications. Categorisation and prioritisation of security requirements will help achieve realistic goals against business targets. For example, for a networked enterprise, we need to separate the enterprise system into two further categories of security requirements such wired and wireless security enterprises. The EC-SQUARE method elicitation of security requirements have been applied to study the behaviour of threat modelling for Enterprise Cloud data security which has been presented in the last section of this chapter.

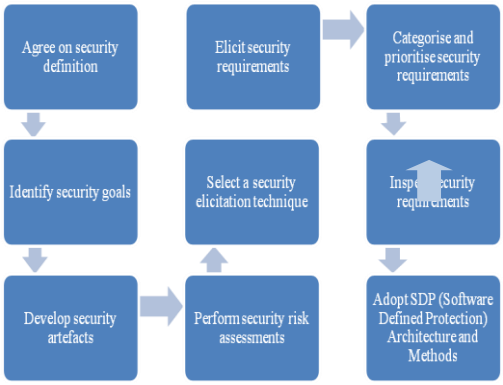

Figure 1. EC-SQUARE Model

D. *Security Attributes*

Enterprise Cloud security attributes are important to Cloud security and our previous work has identified security attributes which belong to the following categories [2, 4]:

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

The above Enterprise Cloud security attributes/characteristics are essential and useful to understand non-functional aspects of services development and service provision. These attributes are also useful for building security in (BSI) and maintaining security. The following section will identify some of the challenges, issues, and opportunities for tackling security-specific

enterprise development and how this can be applied to solve some of the key challenges that are facing Enterprise Cloud computing benefits. The following section will also use Enterprise Cloud security attributes and frameworks identified in this section as the main input for BSI not developing security patches after Enterprise Cloud services has been delivered.

Checkpoint, a software technologies limited, more recently, has introduced the concept of a Software Defined Protection (SDP) for enterprise security blueprint by emphasising the need for a secured enterprise security for dynamic networks and infrastructures. The concept of SDP offers a pragmatic approach to building an enterprise security based on the enterprise architecture and agile methodology. The SDP architecture divides the security infrastructure into three interconnected layers (ESB 2014):

- An Enforcement Layer that is based on physical and virtual security enforcement points and that segments the network, as well as executes the protection logic in high demand environments.
- A Control Layer that analyzes different sources of threat information and generates protections and policies to be executed by the Enforcement Layer.
- A Management Layer that orchestrates the infrastructure and brings the highest degree of agility to the entire architecture.

The SDP, as shown in Figure 2, has been extended with our EC-SQUARE model as discussed in this chapter for a more systematic approach to building enterprise SDP.

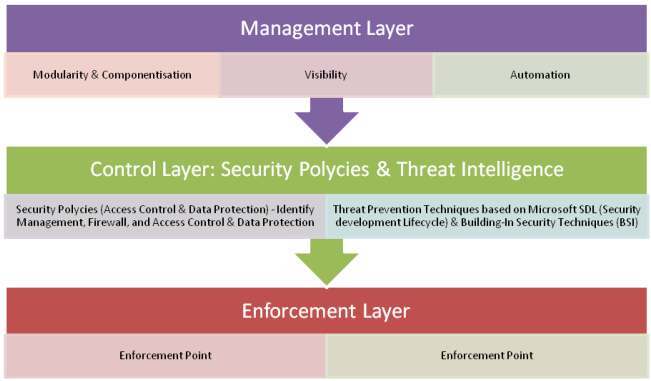

Figure 2. EC-SQUARE SDP Framework

In the context of our EC-QDUARE SDP framework, the management layer provides support for overall management of Enterprise Cloud security for clients as well as in-house. The various modules in this layer are componentised to provide flexibility for making changes and reuse. The control layer provides support for security policies for access control and data protection for the Enterprise Cloud data centres as well as client devices. This layer also supports with threat intelligence based a number of key BSI techniques including SDP. The Enforcement layer supports key enforcement points where a complete profile for each user can be created and analysed securely.

III. Enterprise Security Engineering for Enterprise Cloud Computing: Issues and Opportunities

This section presents discussion for issues and opportunities for Enterprise Cloud Computing. Many security patches have been invented to protect against spam, viruses, id theft, and phishing. Secure applications should be built from start to delivery which will save cost and effort enormously. Figure 1 provides a framework for providing solution to software security challenges and provides a basic means of achieving software security: benefits such as increased trust, integrity and availability; means of achieving this are by using techniques such as requirements elicitation method for software security and by designing secured functions, objects, components, frameworks, and architectures; and its threats are lack of finding software security engineers, additional cost involved, and people's willingness to develop secured applications.

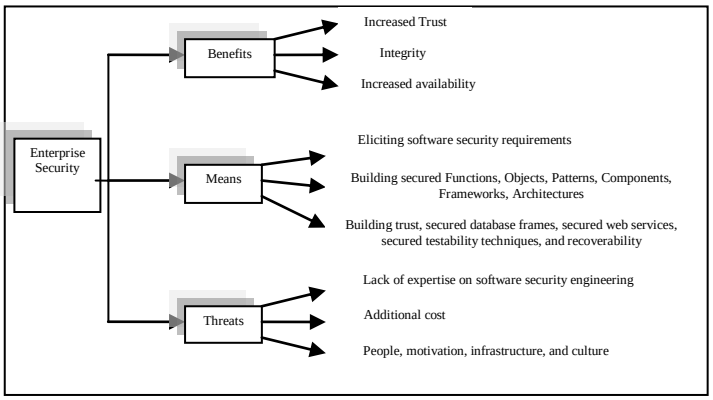

Figure 3. Enterprise security challenges solution framework

Software and Web based applications are growing fast and so the attacks such as virus, phishing, id theft, and spam. In order for us to build trust in web based application users, we should therefore build software security (preventions) as opposed to protection (applying patches soon after attacks have happened in most cases so far in IT industry). *Software security touchpoints* [4] are a set of specific security specific activities to be applied during each software phase in the software development Lifecycle. This includes: (1) identify security requirements and apply abuse cases during Requirements and use cases (phase 1); (2) employ risk analysis during Architecture and design (phase 2); (3) identify risk-based security tests during test plan, conduct tools-based code reviews during coding, conduct risk analysis and adopt penetration testing techniques during the test phase (phase 3) and (4) observe security operations during feedback/release phase. Risk analysis should be conducted across all the phases and need to feedback knowledge gained from attacks and exploitations on a regular basis.

The notion of taxonomy is the practice and science of classification. Taxonomy helps to identify new categories to

shelve and retrieve easily when needed. We know where to find. Castillo [11] defines security as a set of knowledge and tools obtained and developed by means of the observation and the reasoning, systematically structured and of which general principles and laws are deduced to protect the human life and the existing resources. Taxonomy of software security helps to classify techniques and methods, therefore the relevant technique can easily be identified for use. We can also develop a set of specific guidelines which can be used as a checklist for security validation. A kingdom of security considered as a highest group or a top group in the hierarchy. The parameters that affect the kingdom of security are:

- Economical
- Political
- Social
- Functionality

Castillo [11] defines further classify software security engineering and its implementation into two major groups: *software acquisition security* (includes the security specifications in all processes to buy, rent, or interchange software to use in an enterprise) and *enterprises & software development security* (includes the security specifications in all processes to develop information enterprises).

Srinivasan et al. [12] discusses a number of key security taxonomies and challenges for Enterprise Cloud computing. They have divided Enterprise Cloud security into two broad areas: 1) Architectural and Technological Aspects were issues of logical storage segregation and multi-tenancy security issues, identity management, insider attacks, virtualisation and cryptography issues are highlighted; and 2) Process and Regulatory-related issues where governance, insures APIs, SLAs and Trust Management, and Enterprise Cloud Migration issues are identified. These two categories are the key to Enterprise Cloud security challenges. This paper has devoted to addressing Enterprise Cloud data security as the key factor for determining Enterprise Cloud technology. This paper highlights most of the issues and has also provided a number of systematic approaches and solutions to address issues and opportunities including 1) the selected frameworks for Enterprise Cloud security and 2) discussion of the Enterprise Cloud data security with protection mechanisms.

Security-specific enterprises development process methods and techniques shown in this section helps to achieve BSI to traditional enterprises as well as Enterprise Cloud computing applications which needs to be engineered to reap benefits of Enterprise Cloud technology. Our presented work has considered Amazon Enterprise Cloud services as an example for studying the performance of Enterprise Cloud data security. The main reason for choosing Enterprise Cloud data security is that there is little research on this very important issue and data is one of the main reasons that hinders Enterprise Cloud users with respect to building trust.

This section emphasises a rule of thumb to *categorise Enterprise Cloud design principles at the heart of Enterprise Cloud computing as a core principle of service design* when dealing with developing Enterprise Cloud services. Figure 4 shows a model of the pillars of Enterprise Cloud computing with a triangular model. The central focus is Enterprise Cloud security and data security with corner one as scalability, availability, elasticity, and discoverability of Enterprise Cloud services, corner two for service reuse and integrity, and corner three for measuring and continuously improving security and performance assessments of Enterprise Cloud services.

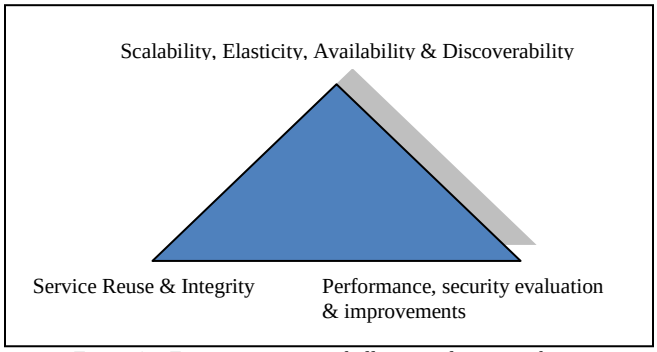

Figure 4. Enterprise security challenges solution attributes

This model provides a framework for integrating data security and developing build-in Enterprise Cloud security systematically. For example, how do we develop a continuous monitoring strategy for Enterprise Cloud identify management and how do improve from failures? This is one the key aim of this model to build on from experience and user feedback and trails in order for Enterprise Cloud providers to be in a sustainable business of Enterprise Cloud computing. We also need a process by which this model can be established when developing and delivering Enterprise Cloud services. In particular, our aim is to build security in (BSI) right from beginning of service development.

IV. DISCUSSION

Section III presents issues and opportunities for Cloud Enterprise security and the selected frameworks including their approaches to the problems and recommendations. This section presents our proposed framework that can address all the issues and concerns described in Section II and III. The Figure 5 shows a process model framework for developing Enterprise Cloud services with BSI simultaneously when developing Enterprise Cloud services. As shown in Figure 5, Enterprise Cloud service development are classified into a number of phases: (1) requirements engineering for Enterprise Cloud services during which time we can identify security related requirements from various stakeholders; (2) conduct business process modeling and simulations (BPM) for each Enterprise Cloud services during which time we can also simulate security aspects and study performance related measures and also introduce a possible number of intrusion and conduct simulations before actual service implementation take place; (3) identify SLAs identifies a number of service level agreements and regulatory and governance related compliances during this time we should be able to separate out security related SLAs and risks; (4) design and develop services during this phase we can

actually implement security related threads that have been carried continuously from all phases, and finally 5) test and deploy services that are developed with BSIs.

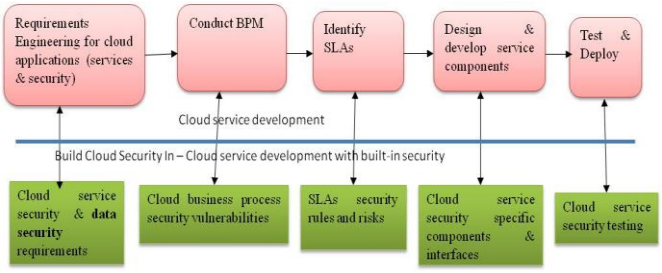

Figure 5. Enterprise Cloud security-based service development and integrating data security process with build-in security

Additional benefits of this approach include:

- Apply software security engineering techniques all identified Enterprise Cloud services. This includes using security analysis tree and various other techniques specified by [8].
- The second step is on identifying BPM (Business Process Modelling) which should include software security analysis for each business process identified to allow us to identify potential security threats which start with service requirements and business requirements as the input to conduct service security analysis using techniques such as Enterprises Secure Quality Requirements Engineering (EC-SQUARE), and Microsoft Secure Development Lifecycle (SDL). The outcome of this process should yield a set of Enterprise Cloud services security requirements with clear indication of software security issues.

V. CONCLUSION AND FUTURE WORK

Enterprise Cloud computing is increasingly in demands since it has established its businesses and software as a service paradigm. However, this new trend needs to be more systematic with respect to software engineering and its related processes. For example, current challenges that are witnessed today with cyber security and application security flaws are important lessons to be learned. This means that best practices for Enterprise Security should be adapted. Similarly, as the demand for Enterprise Cloud services increases and so the increased importance sought for security and privacy. Enterprise Cloud application security can be used from the start of the Enterprise Cloud service development. Enterprise Cloud computing is a multi-disciplinary that includes social engineering, software engineering, software security engineering, distributed computing, and service engineering. Therefore, a holistic approach is needed to build Enterprise Cloud services. Use Business process modelling and simulation to study service and business performances before implementation.

Before Enterprise Cloud computing has established its businesses and software as a service paradigm is increasing its demand for more services. However, this new trend needs to be more systematic with respect to software engineering and its related processes. For example, current challenges that are witnessed today with cyber security and application security flaws are important lessons to be learned. It also has provided best practices that can be adapted. Similarly, as the demand for Enterprise Cloud services increases, so do the importance sought for security and privacy increases. We can build Enterprise Cloud application security from the start of the Enterprise Cloud service development. Enterprise Cloud computing is a multi-disciplinary that includes social engineering, software engineering, software security engineering, distributed computing, and service engineering.

REFERENCES

[1] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, "Cloud computing—The business perspective". Decision Support Systems, 51(1), 176-189, 2011.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. A. Pattinson, A. Rabkin, I. Stoica & M. Zaharia, A view of cloud computing. Communications of the ACM, 53(4), 50-58, 2010.

[3] V. Chang, R. J. Walters, G. Wills, "The development that leads to the Cloud Computing Business Framework", International Journal of Information Management, 33(3), 524-538, 2013.

[4] G. McGraw, "Software security: building security in", Vol. 1. Addison-Wesley Professional, 2006.

[5] T. Mather, S., Kumaraswamy, S., Latif, "Cloud security and privacy: an enterprise perspective on risks and compliance", O'Reilly Media, Inc., 2009.

[6] M. A. Smith, R. L. Kumar, A theory of application service provider (ASP) use from a client perspective. Information & management, 41(8), 977-1002, 2004.

[7] V. Chang, M. Ramachandran, "Towards achieving Cloud Data Security with the Cloud Computing Adoption Framework", technical paper.

[8] M. Ramachandran, "Software Security Engineering: Design and Applications", Nova Science Publishers, New York, USA, 2011.ISBN: 978-1-61470-128-6, 2011.

[9] I. A. Tondel, al. "Security requirements for rest of us: a survey", IEEE Software, Special Issue on Security and Agile requirement engineering methods, Jan/Feb, 2008.

[10] N.R. Mead, et. al., "Security Quality Requirements Engineering (SQUARE) Methodology", Technical report, CMU/SEI-2005-TR-009, 2005.

[11] O. Y. G., Castillo, "Securing the Cloud for the Enterprise", A Joint White Paper from Symantec and VMware

[12] K. M. Srinivasan, et al., "State-of-the-art Enterprise Cloud Computing Security Taxonomies: A classification of security challenges in the present Enterprise Cloud computing environment", ICACCI '12, CHENNAI, India, August 03 – 05, 2012.