RESEARCH ARTICLE OPEN ACCESS

Research On Preserving User Confidentiality In Cloud Computing – Design Of A Confidentiality Framework

Harish Chennamsetty
M.Sc. - Software Engineering, Blekinge Institute of Technology (BTH), Karlskrona, Sweden

ABSTRACT
Cloud Computing creates a dynamic resource sharing platform. Using cloud technologies such as virtualization, data can be provided to the active users who are at high need to utilize the resources provided within the cloud. As this data (or service) is stored (or offered) outside the data owner's boundaries, they are skeptical for utilizing cloud technology in order to store or utilize their data or service. There are many issues for these active clients (companies or individuals) to be petrified at the thought of using cloud computing paradigm. Some of the main issues that make the clients not to choose cloud computing may be determined because of three important security aspects such as confidentiality, integrity, and availability. This research focused on the security models that relate confidentiality issues. A literature Review is performed for analyzing the existing confidentiality frameworks and security models in the area of grid computing, cluster computing and virtualization. A new theoretical framework is then designed to overcome confidentiality issues thereby improving the client'sgeneric understanding of cloud computing services. The resulting framework when implemented in real world would motivate clients to transform their businesses on to cloud.

I. INTRODUCTION

Cloud computing evolves to be a consistent term with collaboration of various IT technologies involved in it [15]. Resource pooling technology in cloud computing paradigm renders the ability to store and dynamically allocate space to the resources that occur for storage periodically[15]. Virtualization technology[6] in cloud computing paradigm renders the ability to run resources that dynamically scale the user's necessity and share the resources available to support the need[15]. Datacenterswith resource pooling technologies [8][15]act like a 'cloud' whereas the concept of 'provisioning services in a timely (near on instant), on-demand manner, to allow the scaling up and down of resources' generates a virtualization mechanism which pretends to be 'computing'[15]. Hence, 'cloud computing' deserves to be a collective term of several technologies that interrupt effectively for dynamic allocation/de-allocation of resources[15]. The generally accepted standard definition[15] of cloud computing is published by the National Institute of Standards and Technology (NIST). Their published[1]definition is used in our research.

In short, to describe NIST definition[15], we understand that, the convenient and ubiquitous network access creates a moderate effort to motivate clients in establishing their resources on to the cloud. The shared pool of configurable computing resources contribute an Instant allocation/de-allocation of resources that occur for on-demand data access [15]. Rapid provisioning provides a flexible operation of cloud for the cloud providers to scale the resources by assigning and releasing resources from time to time when they are required elsewhere[15]. A brief overview of virtualization in cloud computing is provided in the below figure-1.

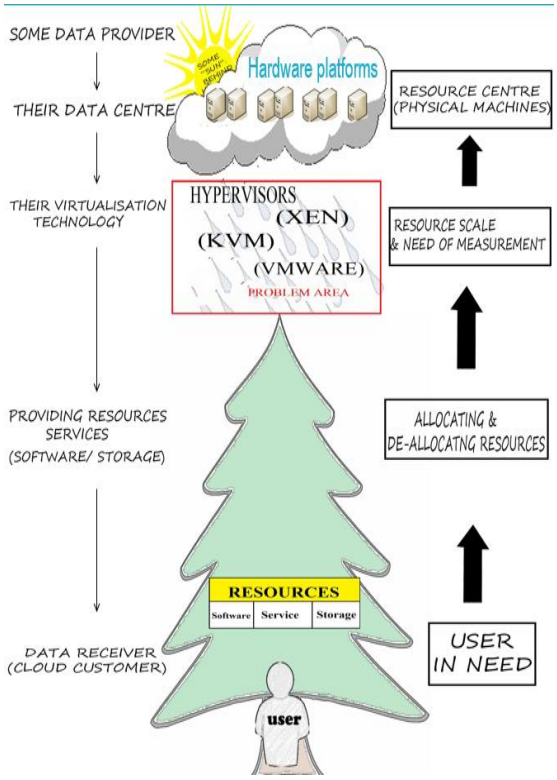

Figure 1: Concept of Virtualization in Cloud Computing

[1] NIST def: http://www.nist.gov/itl/csd/cloud-102511.cfm

As the technologies keep intruding into cloud computing paradigm, there is no means to say cloud computing is exhaustive. Cloud computing key-characteristics, models and implementations are more extensively discussed in Section-II. The security issues increased overtime along withthe raise of cloud computing[2][2]. This resulted in the lack of confidence in client to move their services to cloud [10]. Potential clients are now waiting for the answers about how, why and by what means the security is provided with cloud computing[2].

The problem is distinct as the security issues occur frequently in parallel to the cloud development. The environment of cloud computing is vast making it more vulnerable to threats[2]. Hence, this research focused on the most eminent security issues that significantly standardize the usability, confidentiality and adaptability of cloud computing to a better extent. It is believed that when this problem area is addressed, approximately at least a near half of the security issues should find possible solutions. Clients and developers should be able to come toa common understanding on the cloud services.

The data behind the cloud is technically said to be off-premise and is never under the boundaries of the data owners[8]. Further, data that are stored in cloud are beyond the control of data owners which may converge with loss of confidentiality[2]. Hence, the goal of this research is to generate a successive framework for cloud computing that can predict sufficient confidentiality gain, usability, adaptability and common understandings between developers and clients.

The objective of this research is defined in Section-III. The problems (that may generate during the implementation of the resulted framework), the limitations and the sustainable arguments to our study are brought-up to note in section-IV. Our final research results that are concerned with our research goals are presented to acknowledge our study in conclusions part (section V, VI and VII).

II. BACKGROUND AND MOTIVATION

The security issues such as *Confidentiality; Integrity; Availability;* are indefinitely implemented to reach the efforts constraining to healthy on-demand network access[2].Thus, these efforts when indistinct may route to problems in cloud service models (such as *SAAS; PAAS; IAAS;*) which when left unsolved might cause lack of proficient security (CIA)[2][7]. One of the main reasons for cloud computing to be inconsistent in confidentiality is due to differences in cloud models that are getting deployed [2]. The three deployment models (*Public Cloud; Private Cloud; & Hybrid Cloud;*) generate a multiple framework activity that has to be satisfied with confidentiality[7].

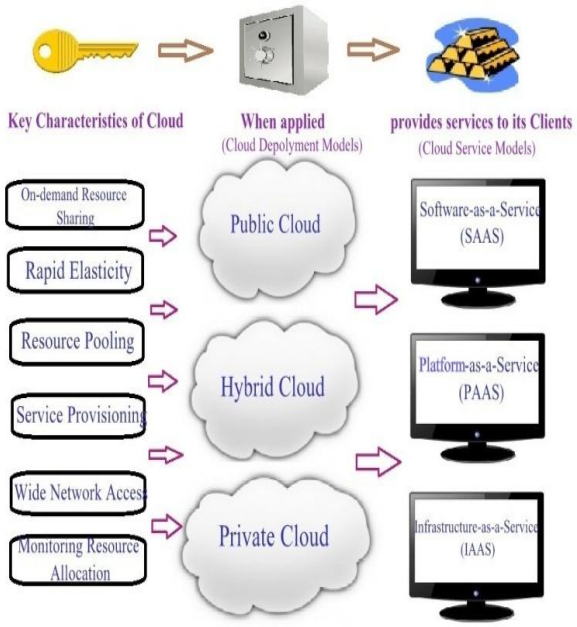

Figure-2: Understandings NIST [15] definition

The NIST definition is supported by five key cloud characteristics, three delivery models and four deployment models [15]. We understood this definition as of three interlinking properties of a cloud: key characteristics of a cloud, delivery models and deployment models. Our understandings on this definition are presented in Figure-2.

The key characteristics describe the operations performed in a cloud computing environment. The key characteristics such as *on-demand resource sharing; resource pooling; rapid elasticity; monitoring resource allocation; wide network access; service provisioning;* has elaborated the cloud technology in detail [15].The cloud service models such as *Software-As-A-Service (SAAS); Platform-As-A-Service (PAAS); Infrastructure-As-A-Service (IAAS);* are said to be general classifications of the cloud [15]. Regardless of the service models that are classified, there exist 3 basic deployment models of cloud such as *public cloud; private cloud; and hybrid cloud.*"Hence, the key characteristics of cloud when applied (to deployment models), provide data or services to its clients."

Here,confidentiality issues underlie the challenges in finding answers to questions listed below that indeed worked as a partial hypothesis for this research:

- How will cloud provisioning occur to act?
- What are cloud security requirements?
- How will data storageoccur in cloud computing?
- How reliable is security architecture of the cloud?
- How reliable are the cloud services offered?

[2]Info-graphic http://imgur.com/yFfAU (dated:15Sep2015)

We are focused to propose a unique framework that can produce a single architecture which allows combination of required security goals along with all the reliable policies, procedures for all cloud deployment models in common. So, we further continued our research on classifying the security issues that are analyzed from our background results.

With the understandings we have - upon the found security issues, we now classified them as the issues that relate to confidentiality with one among the three, they are:

Classifying Security Issues in Common
Technical issues
Organizational issues
Legal issues

The entire list of security issues are generalized into these three issues in common. This complete list of security issues obtained in background is presented in Appendix-A.

Our reasoning for the above classification is as follows.

Technical issues. All the security issues like 'shared technology vulnerabilities', 'network security' and many othersthat can find solutions by framing security goals in technical area are analyzed as Technical issues.

Organizational issues. All the security issues like 'malicious insiders', 'data location transparency' and many others that can find solutions by framing security goals in organizational area are analyzed as organizational issues.

Legal issues. All the security issues like 'policy based or procedural based problems' and many others can get the solutions byframing security goals in this area are sorted to be legal issues.

The basis of this classification is just to unite all the security issues relevant to confidentiality in cloud computing. The main idea besides this type of classification is -'if we unite all the confidentiality issues in common, then we can easily map them onto our framework that is going to be generated.'

A framework like this would help understand the cloud technologies better both in the developer and client's perspective. Furthermore, if we can't find the solution for this research, the implications of not solving this problem might be the same as explained above:

The confidentiality that lacks behind will generate a fear for the clients (companies, organizations, individuals, etc) to share/store their resources (or) to transform their businesses on to the cloud environment.

III. RESEARCH OBJECTIVE

A. Research objective:

The goal of this research is "to generate a sufficient usability, confidentiality and adaptability model (framework) to the extent possible, which when implemented in real-time may moderate the activities (that occur for security threats or implicating risks) that are indeed capable of reducing Confidentiality of the Cloud and its environment."

This Research aim focused our objectives onto:

- Specifying the security issues that relate to Confidentiality in Cloud Computing.
- Understanding the possible research results of the effective security models presented by the previous researchers.
- Proposing a more extensive security model-framework that can uniquely state the province of all service and deployment models in collaboration.

IV. RESEARCH OPERATION

The scope of this research is to present a confidentiality framework that can peer all the service and deployment models present in the cloud. Hence, our major tasks constitute the operations contributing with the minimal tasks of analyzing security issues, generating a framework that architects all the security solutions for the issues generated.

A. Literature Analysis:

In engineering privacy [10], the authors generated three sphere models (*User Sphere; Joint Sphere; and Recipient Sphere;*)that occur for user privacy and confidentiality concerns. They relate all the confidentiality issues to these three spheres. These models are considered as operations that obscure privacy views. They also generated some architectural mechanisms that can also partially generate confidentiality in cloud computing area. These mechanisms are as below:

- *Privacy-by-policy:* Based on policy generation which results in Fair Information Practices (FIP).This FIP was contributed to European Legislation Privacy [10].
- *Privacy-by-architecture:* Based on anonymizing information which results in little or no personal data detection by third parties [10].
- *Hybrid approach:* Based on the combination of above two approaches where policies collide with technical mechanisms (architecture), they then enforce privacy enhancements [10].

These policy centric architectures have given a start to our security framework idea being generated.

In [4], the authors developed security classification framework which sorted the presence of our research idea towards a solution. They classified the security issues for Grid Computing environment also with decentralized data control over its architecture. The Figure 3 presents their framework:

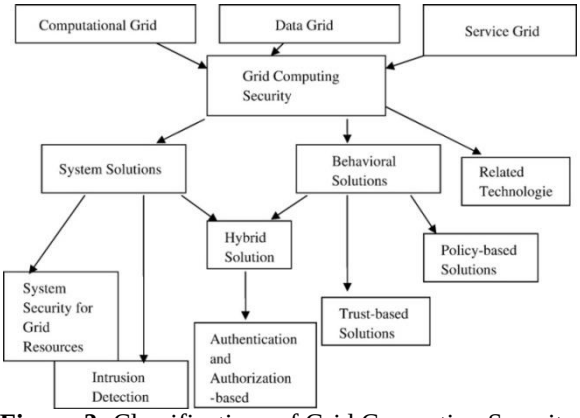

Figure-3: Classifications of Grid Computing Security [4]

As they focused on grid computing, the security issues resulted to solutions in their framework will lead to grid environment's security province but as they interlinked these security issues to grid deployment models (*computational grid; data grid; service grid*;) and as the same security issues (like intrusion detection) can be found in cloud deployment models, their framework helped this research for initiation a framework for confidentiality and adaptability. Moreover, their classification framework also presented the solutions to the issues area-wise (*system solutions, behavioral solutions, hybrid solutions*). In the same way, we focused our solutions to the confidentiality issues area-wise where they are named as technical solutions, organizational solutions and legal solutions.

In 'Cloud Security Issues' article [2];B. R. Kandukuri*et al*., described several Service Level Agreements (SLAs) for generating notion to different levels of security. According to them SLAsare documents that define relationship between two parties such as the cloud provider and the customer (recipient). This concept of indulging security risks in the SLA has given a complete understanding of what needs to be done in our framework. The simple analysis of SLA and its contents are like the below.

- Definition of services
- Performance management
- Problem management
- Customer duties and responsibilities
- Warranties and remedies

It is analyzed that these contents when applied into real-world can generate answers for the partial research hypothesis presented above in the Background Section.

To be consciously reading about encryption concepts in many literatures[5] [11]saying that they have generated a mechanism for confidentialitylacked common understanding in the perspective of both client and a developer. They have generated some encryption key-mechanisms, encryption algorithms, cryptography methods and soon which can be sorted like a solution for "data privacy" alone but not to entire confidentiality measures in security framework. It is believed that only a key generation concept might not itself offer confidentiality. As said by S. Spiekermann et al.,[10] the user is out of the boundaries of the organizational sphere where these keys get generated, and so, even though the key is set private to the users themselves, we can't find any proof to say that these consistent key encryption mechanisms alone can stabilize confidentiality requirement in cloud environment.

A new concept said to be *RAIN(Redundant Array of Independent Net-storages) [9]* has been analyzed from the literature. According to the authors [9], a divide and conquer method for the data passing through the clouds could be used. They have also presented their background work of deploying 5 cloud service models. They are as shown below.

- *Separation model:* separates data storage from data processing[9].
- *Availability model:* separates stored data from data providers during the time of processing[9].
- *Migration model:* describes the data migration from one storage provider to other storage provider[9].
- *Tunnel model:* describes data tunneling service between data processing service and data storage service[9].
- *Cryptography model:* describes data encryption that is also not intelligible even to the storage provider[9].

Their procedural implementation provided an idea forthe framework that implements process activities one-onto-one presenting itself as security control-flow architecture.

In another paper named 'understanding Cloud Vulnerabilities' [1], the authors have generated a framework mitigating the Risk factors into two kinds, "loss event frequency" and "probable loss magnitude", all the rest are classified into these two risk factors. This can be seen as of a relevance to our security issues generalization concept; for mapping them into the framework that can give solutions to any kind of issues that occur in the *open risk taxonomy*[1].

As to conclude with the literature review analysis, the solutions that are obtained provided some source to answer our research problem. This review has shown the relevant security threats or risks or issues that are interlinked with the security models but for complete solution of R.Q.1& R.Q.1.1, we also considered a few NIST drafts that enabled the Risk analysis process or frameworks consistent with cloud environment. The below are the knowledge gained concepts from different drafts of NIST.

In NIST Draft SP800-30 [12], risk assessment methodology flowchart is presented with explanations for each concept beneath the Risk taxonomy and its control flow. The nine steps that determine the sequential flow are as follows [12].

Step1: System characterization
Step2: Threat identification
Step3: Vulnerability identification
Step4: Control analysis
Step5: Likelihood determination
Step6: Impact analysis
Step7: Risk determination
Step8: Control recommendations
Step9: Results documentation

This framework is as shown in Figure-4 below. With elaboration, NIST Draft SP800-37 [13] has further presented a risk management framework which became the key to this finding a solution.

In NIST draft SP800-125[14], the architecture of virtualization technologies is enabled with *hypervisors* that have played a major role for providing security to the cloud computing environment. The security controls when operated in the hypervisors (virtual machine managers for monitoring multiple hosts) that are placed just before the cloud offering applications can implement controlled security operations for this environment.

Even though deployment models exist, a general scope and control flow of the service models in cloud computing with the views of both consumer and cloud provider are presented in Draft SP800-144[16]. This scope in terms of control flow is thus also implemented by us where the cloud provider's view and the customer's view on the framework being generated are extracted to act.

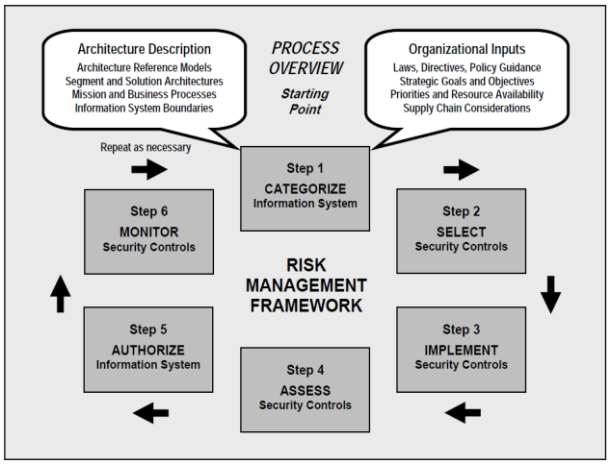

Figure-4: Risk Assessment Framework (NIST SP80037) [13]

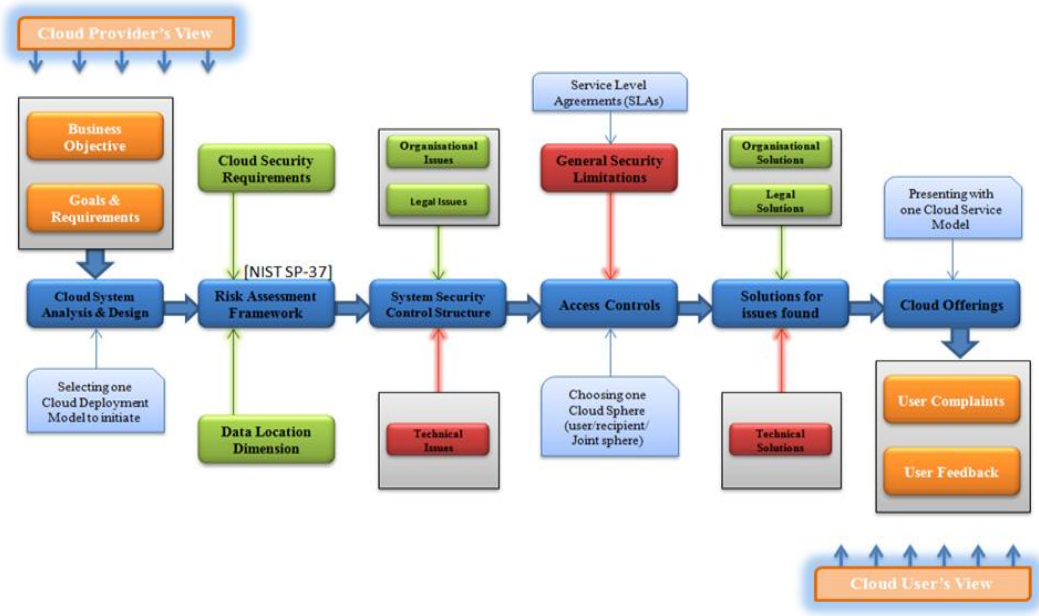

Figure 5: Confidentiality Framework for Cloud computing (our research solution)

Hence, our research problem is completely fulfilled with knowledge base of security issues as shown above with relevance to security models that are deployed to eradicate trouble caused by these issues.

V. DATA ANALYSIS AND INTERPRETATION

Even though there are many other security models or frameworks, only the important articles are presented. As the knowledge for relevant data models got its place for our idea creation from among these articles, hence, the literature review for analysis is concluded. A data framework activity thus resulted in presented in this section. The framework that satisfies our research problem is contributed to effect from the FIGURE-5 below.

This Framework is done in such a way that cloud providers and their customers have a generalized view on the security operations in their cloud. The framework has also shown the difference between the operations that are carried for stepwise flow. For differentiating and clubbing several operations carried in the cloud, orange, blue green and red colors are used. All the orange boxes denote the general tasks by the cloud provider or their customers. All the blue boxes denote the original security operational flow in the framework. Green and red denote the organizational and technical issues/tasks respectively. The description of this tasks and operations will refer back to the review made in Section-IV. Furthermore, a brief explanation for all security concepts and other keywords used in the below framework are clearly elaborated in Appendix-B.

VI. DISCUSSIONS

B. Contributions& limitations :

The framework has deployed a risk management activity for security provisioning in cloud environment. We aresure that results generated are completely involved with all the levels of security issues and their solutions in all kinds of users' views; and hence, will provide a constant baseline for drawing security architecture in any cloud based company that indeed can satisfy the cloud customers. Even though just a literature review can't deal with the entire problem area and also as there is no proof that the resulted analysis can work in the real time industry, with time constraints that concern this research, there is no other choice other than to design the Framework purely based on the theoretical validity obtained fromthe literature review. This framework is limited to the general activities without concise on any further clarifications on the inside elements such as cryptography and soon.

C. General proceedings(future work):

As of now this model needs to be scrutinized based on future experiments with framework under implementation, focus groups with experts detailing the possibility of our theoretical framework in real-time industry. This model needs to be briefly elaborated deriving each and every activity in the framework analytically with real-time proof of concept which is left as a future work. The real-world validity could be obtained with the help of real time industry practitioners, other cloud and security researchers that get involved inempirical survey(s) and experiment(s) conducted.

VII. CONCLUSION

Confidentiality for Cloud Computing deals with the emerging cloud architectures that evolve with time. This continuous evolution process might necessitate to with stand a baseline framework activity. A framework activity with reference to general security models and patterns is resulted with this research. This framework is expected to be a consistent approach to trigger any kind of security mechanism in Cloud Computing. As the views on this model are focused to analysis with both Cloud provider and the customer, organizations may be at ease to implement their operations directly on to this framework without any further setbacks.

REFERENCES

[1]. B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security & Privacy Magazine*, vol. 9, no. 2, pp. 50–57, Mar. 2011.

[2]. B. R. Kandukuri, R. Paturi. V., and A. Rakshit, "Cloud Security Issues," 2009, pp. 517–520.

[3]. C. Chapman, W. Emmerich, F. G. Márquez, S. Clayman, and A. Galis, "Software architecture definition for on-demand cloud provisioning," *Cluster Computing*, vol. 15, no. 2, pp. 79–100, Feb. 2011.

[4]. E. Cody, R. Sharman, R. H. Rao, and S. Upadhyaya, "Security in grid computing: A review and synthesis," *Decision Support Systems*, vol. 44, no. 4, pp. 749–764, Mar. 2008.

[5]. G. Zhao, C. Rong, J. Li, F. Zhang, and Y. Tang, "Trusted Data Sharing over Untrusted Cloud Storage Providers," 2010, pp. 97–103.

[6]. K. Riemer and N. Vehring, "Virtual or vague? a literature review exposing conceptual differences in defining virtual organizations in IS research," *Electronic Markets*, May 2012.

[7]. K. 'Shade O, I. Frank and A.Oludele, "Cloud Computing Security Issues and

Challenges,"*Journal of Network and Computer Applications*, vol. 3, no. 5, pp. 247-255, Dec. 2011.
[8]. M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, p. 50, Apr. 2010.
[9]. M. G. Jaatun, G. Zhao, and S. Alapnes, "A Cryptographic Protocol for Communication in a Redundant Array of Independent Net-storages," 2011, pp. 172–179.
[10]. S. Spiekermann and L. F. Cranor, "Engineering Privacy," *IEEE Transactions on Software Engineering*, vol. 35, no. 1, pp. 67–82, Jan. 2009.
[11]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," 2010, pp. 1–9.
[12]. *NIST Special Publication (SP) Drafts:*[Online]
[13]. (Available:http://csrc.nist.gov/publications/PubsDrafts.html)
[14]. S. Gary, G. Alice, and F. Alexis, "SP: Risk Management Guide for Information Technology Systems," *National Institute of Standards and Technology (NIST)*, CSRC-SP 800-30, July. 2002.
[15]. "SP: Guide for Applying the Risk Management Framework to Federal Information Systems,"*National Institute of Standards and Technology (NIST)*, CSRC-SP 800-37(Rev-1), Feb. 2010.
[16]. S. Karen, S. Murugiahand H. Paul, "SP: Guide to Security for Full Virtualization Technologies," *National Institute of Standards and Technology (NIST)*,CSRC-SP 800-125, Jan. 2011.
[17]. M. Peter and G. Timothy, "NIST Definition of Cloud Computing," *National Institute of standards and Technology (NIST)*,CSRC-SP 800-145, Sept. 2011.
[18]. J. Wayne and G. Timothy, "SP: Guidelines on Security and Privacy in Public Cloud Computing," *National Institute of Standards and Technology (NIST)*,CSRC-SP 800-144, Dec. 2011.
[19]. *SLR model review references:*
[20]. S. Jalali and C. Wohlin, 'Agile practices in global software engineering - a systematic map', in *2010 Fifth IEEE International Conference Global Software Engineering (ICGSE 2010), 23-26 Aug. 2010*, Los Alamitos, CA, USA, 2010, pp. 45–54.
[21]. Guido Kok, "Cloud computing & confidentiality," M.S. thesis, Dept. Comp. Sci. Eng., University of Twente., Enschede-Noord, Nederland, May.24.2010.[Online]
[22]. (Available: http://purl.utwente.nl/essays/61039)

Appendix A –Secuirty Issues Generalisation (From Background Results)

The security issues that relate to confidentiality are presented here with analysis from our previous studies. As said in the research report, these issues are focused to generalize them into 3 main categories such as Technical, Organizational, Legal issues; as shown in the Table –A below.

Table A: Security issues found in PRE-SLR and our view of generalizing them to 3 main issues

Security Issues	Issues found from PRE-SLR (references)	Issues can Relate to Confidentiality as :-
Abuse and Nefarious Use of Cloud Computing	[R7], [R12]	Technical issue
Account, Service and Traffic Hijacking	[R7], [R12]	Technical issue
Authentication and authorization	[R17]	Technical issue
Cost and Limited availability of technical personals	[R1]	Organizational issue
Customer Isolation and Information Flow.	[R 15]	Technical issue
Cloud Integrity and Binding Issues	[R10]	Organizational issue
Cloud Security vulnerabilities and Security Attacks	[R2], [R10]	Technical issue
Cloud Governance	[R16], [R18]	Legal Issue
Data access and Control	[R17]	Technical issue
Data back-up and recovery	[R2], [R14], [R20]	Technical issue
Data breaches (controlling XML signatures and soon)	[R17]	Technical issue
Data location	[R14]	Organizational issue
Data protection (Loss/Leakage)	[R7], [R12], [R21]	Technical issue
Data provisioning (Audits, etc)	[R2], [R10], [R15]	Technical issue
Data segregation	[R17]	Technical issue
Ensuring user rights (End user Trust)	[R18], [R21]	Legal issue
Federation and Secure Composition	[R15]	Legal issue
Identity/Key management (Encryptions)	[R20]	Technical issue
Insecure Application Programming Interfaces (web application security)	[R7], [R12]	Technical issue
Integrity for user's dynamic changes	[R21]	Organizational issue
Investigative support (data forensics and soon)	[R2], [R16]	Technical issue
legal, policy based and commercial problems	[R18]	Legal issue
Long-term viability (End user trust)	[R2], [R16]	Organizational issue
Malicious Insiders	[R7], [R12], [R15]	Organizational issue
Multi-Compliance Clouds	[R15]	Technical issue
Network security	[R17], [R21]	Technical issue
Non-Repudiation	[R16]	Organizational Issue
Privileged user access	[R14]	Organizational issue
Regulatory Compliance	[R16]	Legal issue
Reliability	[R8], [R20]	Organizational issue
Risk/Threat Management	[R2]	Technical issue
Security assurance to cloud users	[R10]	Organizational issue
Security Integration & Transparency.	[R15]	Technical issue
Shared Technology Vulnerabilities	[R7], [R12]	Technical issue
undefined cloud boundaries	[R21]	Legal issue
Unknown Risk Profile (lack of transparency)	[R12]	Organizational issue
Virtualization vulnerability	[R2], [R17]	Technical issue

NOTE: The references "[R]" refer to the background results references. These references are presented in Appendix-C.

All the security issues presented above that are generalized into these 3 issues are only through our understandings upon them. Along with these existing issues presented above, any future issues that evolve with time or any other issues that are not sighted by us can also be set into one of these 3 issues in the future.

Appendix B–Keywords Used (in the research report)
Cloud Computing & confidentiality (As it is):
Cloud computing (NIST definition)
"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics**,** three service models, and four deployment models." [15]
Confidentiality (NIST definition-FIPS PUB 199)[S15]

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."
Integrity (NIST definition-FIPS PUB 199)[S15]

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."
Availability (NIST definition-FIPS PUB 199)[S15]

"Ensuring timely and reliable access to and use information."

Cloud service models
Software as a service (SaaS)[15]

The SaaS service model is defined to services that render software applications to the cloud customers. Here, if needed, the Cloud provider can also operate these applications instead of customers like application management (updates), storage backups, infrastructure and soon.
Platform as a service (PaaS)[15]

The PaaS service model is derived to offer interfaces such as operational platforms to the cloud customer. These platforms are helpful to the customer in order to build some new applications that are supported on cloud based technologies. Here, the operations such as network management, storage, and operating systems are managed by the cloud provider itself and hence the customer can be relieved to work only for their application development but not in other matters of cloud maintenance.
Infrastructure as a service (IaaS)[15]

The IaaS service model is derived from the concept for reducing costs to the customer. IaaS is structured to provide the capabilities of cloud provisioning, storage management and other fundamental needs to the customer for making them to use cloud technologies. Here, the customer is application or file management is indirectly controlled by the cloud provider.

Grid Deployment models
Computational grid [4]

The concept of separating resources for setting them aside in order to automate the computational works that can reduce computational power and man-power is said to be Computational grid.
Data grid[4]

The information and data are stored or retrieved to analysis from this data grid. This data grid is modeled in such a way that large volumes of data are accessed from single Cloud data centre at a time by several users (or companies or organizations).
Service grid[4]

The grid that offers services to its clients is said to be Service grid. This grid is designed with mechanisms of provisioning customer requirements and offering services they require.

Cloud deployment models
Private Cloud[15]

the services offered are monitored by the organization itself where its services are not shared to be monitored by outsiders for any other purposes, i.e., the physical infrastructure (cloud) may or may not be owned by the organization and might be on-premise or off-premise but will contain a designated service provider (employees or entities) for its cloud computations.
Public cloud[15]

The cloud is provisioned to use by any source that is in need, this source can be an individual, an organization, or some other entity. This cloud is generally maintained by ordinary cloud provider and mechanisms where low-level security is provided for usage.

Hybrid cloud[15]

It is a combination of public or private or any other deployment cloud (such as community clouds) that is designed into single cloud architecture. The user may vary according to the organizational needs and hence the security may also vary with it.

Cloud key characteristics

On-demand resource sharing[15]

The provisioning of services offered can leverage a concept of 'On-demand resource sharing'. This is automated process that enables the control mechanism of reducing human efforts for enabling services to the right users.

Resource Pooling[15]

As delivered to our research report above from NIST, Resource pooling technology in Cloud Computing Paradigm renders the ability to store and dynamically allocate space to the resources to occur for storage periodically.

Rapid elasticity[15]

The rapid elasticity is derived as: provisioning services with capabilities to automatically scale the exact user-demand. The resource is set to use for the demand and this service is reverted back when the customer is not in need of that resource.

Wide network access[15]

The ability to control or mange large area networks is delivered to output by this wide network access. With this characteristic we can be access data or information or service even through mobile devices.

Cloud Spheres models

User Sphere: [10]

The user sphere is a technical domain name which seems to be encompassing a user's device. This sphere has to enable a full access control to the users who own it. The data is set to privacy and is accessible to entities present in external boundaries only with the data owner's permissions. Additionally, user sphere models are trumped with respect to owner's physical privacy and hence, will wait for their interruption to change their access setting when needed.

Recipient Sphere: [10]

In the same way as that of user sphere above, the recipient sphere is a company centric sphere where the organization is responsible for its complete access controls. As the control is within the organization itself, the risk is low when compared to user sphere and so can potentially minimizes the risk of privacy breaches.

Joint Sphere[10]

The joint sphere is also a technical domain term of cloud spheres where this sphere can derive the complete cloud to its privacy by setting the controls completely within the organization and also involving its customers with some limitations to access them. we analyzed that this kind of model is not impossible to see in the real world, as we can see social networking sites where the users has given free of charge for using data storage, email services and many other features but the users should indirectly need to know that the full control of these services is withheld with the company (social networking site) itself but not with the user. Hence the privacy control is derived with the complete understandings of the organizations and its customers involved in joint sphere.

Classification of types of Solutions for issues found in grid computing

System solutions[4]

The system based solutions approach is a concept where the technical issues are to be analyzed for solutions and rectifications. Issues such as accessing grid information, auditing grid functions and soon are set to solutions here. We named them to be technical solutions in our research report for our confidentiality framework

Behavioural solutions[4]

The Behavioral solutions denotes the category where solutions for issues like Immediate job execution, advanced scheduling, job control are sorted out for answers. We named them as Organizational solutions in our research report for our confidentiality framework.

Hybrid solutions [4]

These solutions denote the category that combines all kinds of issues for sorting them to gain hybrid solutions. Here, trust is the fundamental for solving any kind of issue. We did not use this kind of solutions in our framework but instead as trust occurs better with policies and laws, we involved legal issues in our research framework.

Some other keywords from literature

RAIN (Redundant Array of Independent Net-storages)[9]

All the deployment models are split to several independent (non-colluding) storage providers that pretend to be Redundant Array of Independent Net-storages (RAIN). In authors view a single chunk of data doesn't comprise Confidentiality and hence they derive that the data should be stored using one or several cloud storage providers.

Open risk taxonomy[1]

Open risk taxonomy is nothing but generalizing the issues (factors contributing) into much similar generalized issue categories. In this paper [1], the risk focus is divided mainly into two types 'loss event frequency', 'probable loss magnitude' with all the rest of the factors that occur for risk must be falling into one of these categories.

Hypervisors[14]

Cloud Computing evaluates a Concept of 'provisioning services in a timely (near on instant), on-demand manner, to allow the scaling up and down of resources'. This approach of making computing a utility in cloud environment provides an Opportunity to dynamically scale the computing resource that are shared among customers using virtualization technology. Allocating / de-allocating these resources efficiently, is an open challenge that is solved by Hypervisors. They allocation and de-allocation mechanisms are automated through these hypervisors. In addition, we have analyzed that at present: VMware, XEN systems (using XEN hypervisors), Kernel-based Virtual Machine (KVM); implementing their services pretend to be Hypervisors in the real-time cloud computing world.

Keywords that occurred in our Confidentiality Framework

(Clear and extra explanation of each and every word used in our Framework)

Cloud system analysis and design

The system analysis and design is the initial step where we choose the Cloud deployment model [15] and designing the tasks that work upon that model that is chosen.

Cloud security requirements

The general security requirements like key encryptions [5] [11], data storage privacy [8], and many other fundamental requirements should be analyzed before implementing every cloud model. This helps in reducing the risk of cloud failure in security matters. This general look-up what of security requirements needed will somewhat increase the confidentiality in the cloud customers.

Data Location Dimension

Cloud confidentiality fails due to lack of cloud transparency to the customers. Customers are reluctant to transform their businesses on to cloud as they can't see where their data is located and hence, data location dimension distinguishes the data location in data owner's perspective rather than data provider's perspective [10].

System security control structure

The original security model that is designed to operations for cloud security requirements found earlier is developed here in security control structure. All the security issues are analyzed here and further classified into 3 major chunks (technical, organizational, legal) and are sent to be solved by those different departments that are responsible for solving them [4].

Access controls

The Cloud sphere models [10] such as recipient sphere, user sphere, hybrid sphere occur in access control criteria and will work as the same by transforming their responsibilities and concepts in access controls functions. These access controls even though arose from that sphere concept, the main duty is to preserve confidentiality for the data that is being processed in-and-out of the cloud. As soon as we set the access control to one of these sphere, the cloud will adhere the responsibilities of those sphere that is set and will work for the same.

General security limitations

The general security limitations occur from the concept of data provisioning and security controls that are limited to them in NIST draft SP800-125 [14] and NIST Draft SP800-30 [12] respectively. The general security limitations such as enabling encryption techniques; implementation of virtual private networks; implementation of security settings that suit the service level agreements [2] (that render to organizational standards); generating security assurance criteria and soon come under general security limitations concept.

Cloud offerings

The cloud offering is the final step where we choose the Cloud service model [15] and designing the tasks that work upon that model that is chosen.

Appendix C–Included Studies

EXTRA HELPFUL REFERENCES[3] *([S])*

[S1]. C. Alcaraz, I. Agudo, D. Nunez, and J. Lopez, "Managing Incidents in Smart Grids a` la Cloud," in *2011 IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom)*, 2011, pp. 527 –531.

[S2]. C. I. Dalton, D. Plaquin, W. Weidner, D. Kuhlmann, B. Balacheff, and R. Brown, "Trusted virtual platforms," *ACM SIGOPS Operating Systems Review*, vol. 43, no. 1, p. 36, Jan. 2009.

[S3]. D. W. Chadwick and K. Fatema, "A privacy preserving authorisation system for the cloud," *Journal of Computer and System Sciences*, vol. 78, no. 5, pp. 1359–1373, Sep. 2012.

[S4]. H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security & Privacy Magazine*, vol. 8, no. 6, pp. 24–31, Nov. 2010.

[S5]. J. Li, B. Stephenson, H. R. Motahari-Nezhad, and S. Singhal, "GEODAC: A Data Assurance Policy Specification and Enforcement Framework for Outsourced Services," *IEEE Transactions on Services Computing*, vol. 4, no. 4, pp. 340–354, Oct. 2011.

[S6]. J. Hao and W. Cai, "Trusted Block as a Service: Towards Sensitive Applications on the Cloud," in *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2011, pp. 73 –82.

[S7]. L. M. Kaufman, "Data Security in the World of Cloud Computing," *IEEE Security & Privacy Magazine*, vol. 7, no. 4, pp. 61–64, Jul. 2009.

[S8]. P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L. Ben Othmane, and L. Lilien, "An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing," in *2010 29th IEEE Symposium on Reliable Distributed Systems*, 2010, pp. 177 –183.

[S9]. R. Padilha and F. Pedone, "Belisarius: BFT Storage with Confidentiality," in *2011 10th IEEE International Symposium on Network Computing and Applications (NCA)*, 2011, pp. 9 –16.

[S10]. R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," in *2011 IEEE World Congress on Services (SERVICES)*, 2011, pp. 584 –588.

[S11]. R. Seiger, S. Gross, and A. Schill, "SecCSIE: A Secure Cloud Storage Integrator for Enterprises," in *2011 IEEE 13th Conference on Commerce and Enterprise Computing (CEC)*, 2011, pp. 252 –255.

[S12]. S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," in *2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)*, 2010, pp. 693 –702.

[S13]. U. Greveler, B. Justus, and D. Loehr, "A Privacy Preserving System for Cloud Computing," in *2011 IEEE 11th International Conference on Computer and Information Technology (CIT)*, 2011, pp. 648 – 653.

[S14]. X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information security risk management framework for the cloud computing environments", Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010, pp. 1328.

NIST Special Publication (SP) Drafts: [Online]
(Available: http://csrc.nist.gov/publications/PubsDrafts.html)

[S15]. "Standards for Security Categorization of Federal Information and Information Systems," National Institute of Standards and Technology (NIST), FIPS Pub. 199, Feb. 2004.

REFERENCES ([R]) FOR SECURITY ISSUES PRESENTED IN APPENDIX-A

[R1]. D. Carrell, "A Strategy for Deploying Secure Cloud-Based Natural Language Processing Systems for Applied Research Involving Clinical Text," in *2011 44th Hawaii International Conference on System Sciences (HICSS 2011), 4-7 Jan. 2011*, Los Alamitos, CA, USA, 2011, pp. 11.

[R2]. F. B. Shaikh and S. Haider, "Security threats in cloud computing," in *2011 6th International Conference for Internet Technology and Secured Transactions (ICITST), 11-14 Dec. 2011*, Piscataway, NJ, USA, 2011, p. 214–19.

[R3]. Hao Sun and K. Aida, "A Hybrid and Secure Mechanism to Execute Parameter Survey Applications on Local and Public Cloud Resources," in *2010 IEEE 2nd International Conference on Cloud Computing*

[3]26 relevant and available papers are found in which only 11 supported our study relating Confidentiality framework. Here, some extra references (excluding those 11references that are presented in the research report). Those that did not support for our Framework in any kind but helped us in gaining some extra knowledge are presented here.

Technology and Science (CloudCom 2010), 30 Nov.-3 Dec. 2010, Los Alamitos, CA, USA, 2010, p. 118–26.

[R4]. Jen-Sheng Wang, Che-Hung Liu, and G. T. R. Lin, "How to manage information security in cloud computing," in *2011 IEEE International Conference on Systems, Man and Cybernetics, 9-12 Oct. 2011*, Piscataway, NJ, USA, 2011, p. 1405–10.

[R5]. J. C. Roberts II and W. Al-Hamdani, "Who can you trust in the cloud? A review of security issues within cloud computing," in *2011 Information Security Curriculum Development Conference, InfoSecCD'11, September 30, 2011 - October 1, 2011*, Kennesaw, GA, United states, 2011, pp. 15–19.

[R6]. K. Dahbur, B. Mohammad, and A. B. Tarakji, "A survey of risks, threats and vulnerabilities in cloud computing," in *2nd International Conference on Intelligent Semantic Web-Services and Applications, ISWSA 2011, April 18, 2011 - April 20, 2011*, Amman, Jordan, 2011, p. The Isra University.

[R7]. L. M. Vaquero, L. Rodero-Merino, and D. Moran, "Locking the sky: a survey on IaaS cloud security," *Computing*, vol. 91, no. 1, pp. 93–118, Jan. 2011.

[R8]. L. Sumter, "Cloud computing: Security risk," in *48th Annual Southeast Regional Conference, ACM SE'10, April 15, 2010 - April 17, 2010*, Oxford, MS, United states, 2010.

[R9]. Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, and Aoying Zhou, "Security and Privacy in Cloud Computing: A Survey," in *2010 Sixth International Conference on Semantics Knowledge and Grid (SKG 2010), 1-3 Nov. 2010*, Los Alamitos, CA, USA, 2010, p. 105–12.

[R10]. M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *2009 IEEE International Conference on Cloud Computing (CLOUD), 21-25 Sept. 2009*, Piscataway, NJ, USA, 2009, p. 109–16.

[R11]. M. Townsend, "Managing a security program in a cloud computing environment," in *2009 Information Security Curriculum Development Annual Conference, InfoSecCD'09, September 25, 2009 - September 26, 2009*, Kennesaw, GA, United states, 2009, pp. 128–133.

[R12]. M. T. Khorshed, A. B. M. Shawkat Ali, and S. A. Wasimi, "Trust issues that create threats for cyber attacks in cloud computing," in *2011 17th IEEE International Conference on Parallel and Distributed Systems, ICPADS 2011, December 7, 2011 - December 9, 2011*, Tainan, Taiwan, 2011, pp. 900–905.

[R13]. M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," P.O. Box 211, Amsterdam, 1000 AE, Netherlands, 2012, vol. 28, pp. 833–851.

[R14]. P. Jain, D. Rane, and S. Patidar, "A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment," in *2011 World Congress on Information and Communication Technologies (WICT), 11-14 Dec. 2011*, Piscataway, NJ, USA, 2011, p. 456–61.

[R15]. R. Glott, E. Husmann, A.-R. Sadeghi, and M. Schunter, "Trustworthy Clouds Underpinning the Future Internet," in *The Future Internet*, Berlin, Germany: Springer Verlag, 2011, p. 209–21.

[R16]. S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in Cloud computing," in *2010 Information Security for South Africa (ISSA 2010), 2-4 Aug. 2010*, Piscataway, NJ, USA, 2010, p. 7 pp.

[R17]. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[R18]. S. Tabet and M. Pohlman, "Cloud Computing: Combining Governance, Compliance, and Trust Standards with Declarative Rule-Based Frameworks," in *Rule-Based Modeling and Computing on the Semantic Web. 5th International Symposium, RuleML 2011 - America, 3-5 Nov. 2011*, Berlin, Germany, 2011, p. 230–6.

[R19]. Tsung-Hui Lu, Li-Yun Chang, and Zhe-Jung Lee, "Integrating Security Certification with IT Education," in *2011 International Conference on System Science and Engineering (ICSSE), 8-10 June 2011*, Piscataway, NJ, USA, 2011, p. 582–7.

[R20]. Xin Yang, Qingni Shen, Yahui Yang, and Sihan Qing, "A Way of Key Management in Cloud Storage Based on Trusted Computing," in *Network and Parallel Computing. 8th IFIP International Conference, NPC 2011, 21-23 Oct. 2011*, Berlin, Germany, 2011, p. 135–45.

[R21]. Xue Jing and Zhang Jian-jun, "A brief survey on the security model of cloud computing," in *2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES 2010), 10-12 Aug. 2010*, Los Alamitos, CA, USA, 2010, p. 475–8.

[R22]. X. Lin, "Survey on cloud based mobile security and a new framework for improvement," in *2011 International Conference on Information and Automation, ICIA 2011, June 6, 2011 - June 8, 2011*, Shenzhen, China, 2011, pp. 710–715.