International Journal of Engineering& Scientific Research
Vol.9Issue 10, October 2021
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Secured Threat Modeling Frameworks for Cloud Computing Environment

Shailaja Salagrama*

Abstract

Cloud security and privacy are highly influential to adopt the cloud service. Service providers always try to provide high level of security and privacy as dictated by the customers. Major bottleneck with the service provider is that they have the in-built solution which does not offer the on-demand security and privacy solutions with regional legislation of the privacy regulation. This disables the customers to adopt or host the software service to the cloud environment. In this paper we propose a solution by following the software development life cycle model to develop the on-demand security and privacy requirements dictated by customers of the cloud services. A secured model framework for the design and development of the cloud software as per the customer regional requirements of data privacy with respect their regional legislation and regulation. A systematic development model is proposed under the secured model framework for the cloud environment.

Keywords:

Elastic Computing Service
Cloud Computing Environment
Cloud Governance
Security and Privacy
SDLC,
Legislation and Regulations

Author correspondence:

Shailaja Salagrama,
Student, Phd, Information Technology.
University of the Cumberlands, Williamsburg, Kentucky, USA,

1. Introduction

Cloud computing environment has more risks of threats and unauthorized disclosure of business sensitive and critical information. The network platform such as Internet is public network which is the backbone network mode to access the virtual resources in the cloud environment. Internet is fully insecure network so that more risks of the disclosure of the sensitive information always be a problem to the organizations which has the cloud environment for the information system. Basically, there are three different categories of cloud environments. These cloud services are private, public and hybrid. A private cloud is owned and managed by a particular organization whereas a public cloud is public in nature and any organization can use this by paying rent for accessibility. Hybrid cloud is mixture of private and public cloud environment. Cloud offers three different types of services to its clients. These three services are infrastructure as a service, platform as a service and software as a service. For example, Amazon ECS provides the infrastructure as services to its users. Microsoft Azure and IBM cloud are common platform as a service for the client and Google docs and Microsoft Sharepoint are common software as a service for cloud computing

Threat and its associated risks are major problem with cloud as it may cause the serious damage of business continuity and become the cause of trust loss due to disclosure of the sensitive information related to any stakeholders and process of the organizations. Therefore, it is necessary to reduce the risks and exposures of the cloud resources and assets to the business entities who are clients of the cloud services for any one of three different categories of cloud types. Development of secured software to design the threat model is very important factor for the cloud services. The threat model must have the capability to identify the attacks and propose the counter measure to restrict the exploitation through the vulnerabilities of the system [1]. It is also fact that privacy and security of the information system components and sensitive information are core for any type of security framework and model. The existing security model and frameworks of the cloud environment is not totally addressing the privacy in the cloud computing. Service providers of different types of cloud as mentioned earlier can access and use the information of an organization which client of the cloud

*Doctor of Philosophy, Computer Information System, University of the Cumberlands, Williumberg, Kentucky, USA

services. Therefore, a full proof security framework must be in place to address all the concerns related to privacy of the client and its business-critical information is very much required.

A cloud security threat model with the methodologies having the privacy management to reduce the risks and exposures for both security and privacy must be deployed over the cloud service client information system environment to manage the security and privacy of assets and critical information. A Meta model to identify the privacy threats should be added in the security framework model to enhance the existing security framework to secure the cloud assets. This new proposed designed security framework of cloud has the more robust methodological support to privacy legislation and regulation for cloud service providers and also to the clients of cloud services. The security framework must have the security and privacy management control to address both the issues with single view by inclusion of the legislation and regulation with the threat prevention model. This enhances the security and privacy of the cloud data and users of the cloud computing environment. Also, the trust over the cloud environment with scope of the sensitive information to the organization going to adopt the cloud services would be increased.

2. Secure Threat Model Framwork Characteristics

Software system that works with cloud system should be security preserving with the privacy scope by legislation and regulation. The primary idea behind this new model framework of security is to include the privacy regulation under the software system which handles the threat identification, countermeasure and finally eradication. The design approach of security framework model to provide the security as well as privacy of the cloud data and client cloud assets is the extension of the separate security model framework.

2.1 Inclusion of Privacy Legislation

Key concern is directly related to design such as secured model framework which protects the personal and sensitive information of entities of cloud environment. It is also considered that inclusion of the privacy legislation and regulation to the cloud clients and the software team is very much complex thing. This is due to fact that the regulations and information technology are two different domains of the studies. Further, it is also true that existing security models and frameworks have not included the privacy regulation so that to include this with existing framework leads too much ambiguity and bugs in the system. The solution for this problem is to first identify all the privacy concerns and then model a framework relevant to the existing framework step by step.

2.2 Cloud Service Model with technical Deployment Framework Model

Technical deployment model offers three services such as infrastructure, platform, and software. These all deployments of the cloud offer the rent-based services to the customers or clients. On demand storage, computing and networking resources are also deployed to serve the customers with use and pay basis [2]. The services of the cloud can be provided by the service providers through different deployments such as private, public and hybrid. These all-deployments models are independent to each of the service providers but, some of the deployments such as data storage; virtual machines etc are further handed to the third party.

2.3 Requirements of Customers

Customers or clients of the cloud services are important parameters, and their needs must be in place with the service providers. The project which is agreed with the service provider and client should have to include the customer from beginning of threat modeling to satisfy the customer with the agreed services of cloud. The engagement of customer from early stage of the design and development of threat modeling to secure the sensitive cloud data should have to be clause based and follow all the clauses as per the prior agreement with both parties to follow during the whole project.

3. Model Framework Methodology Parameters

3.1 Model Usability

Cloud provides the less costly options to the customer organizations by providing the IT tools and customer centric release of high quality on demand software in cyclic fashion. The mechanisms and processes used to develop the threat framework must have to be compatible and fast to provide the high level of usability to the customers. Therefore, it is challenging tasks to the cloud service provider to provide the balance between the management of required level of security and privacy with firmly satisfactory demand of customers. The challenge of given demand of customer always tricks the cloud service provider to make the prototype of requirement model to follow from beginning to end of the project required by the customer to be deployed by service provider.

3.2 Threat and Risk Traceability

Identification of threats is very much difficult tasks to the developer of the service provider of cloud. Each identified threat must be documented from early stage to final stage of the service software development. Also, identified threat that is document should be traceable with respect to security and privacy requirements of the customers. This paradigm to trace the threat by inclusion of security privacy requirements of customer viewpoints provide an efficient model to real requirements and further becomes ease to the service provider the change during the post requirement like in the design, implementation and validation processes.

4. Model Framework Methodology Design

Design of model framework for security and privacy are two different aspects of the methodologies, so that a single methodological process cannot fulfill the whole activities related to required development. The demands of specific customer organization require constructions of different methodologies to provide the fulfillment of requirements as demanded [3]. The methodologies to model the framework of security and privacy with service provision as agreed between the service provider and cloud service customer organization is completely based on the design, construction and adapting the methods techniques along with the tools for the project related to secured information system [4]. Ad-hoc methodology is best option to develop the secured software as required by the customer organization. This methodology provides the development from scratch [5][6]. There are also many other methodologies and approaches to develop secured software for the customers. These are paradigm based, extension based and assembly based.

We propose our secured development methodologies which includes the model for highly secured phases of software development life cycle. Model of this proposed methodology is presented by the figure 1.

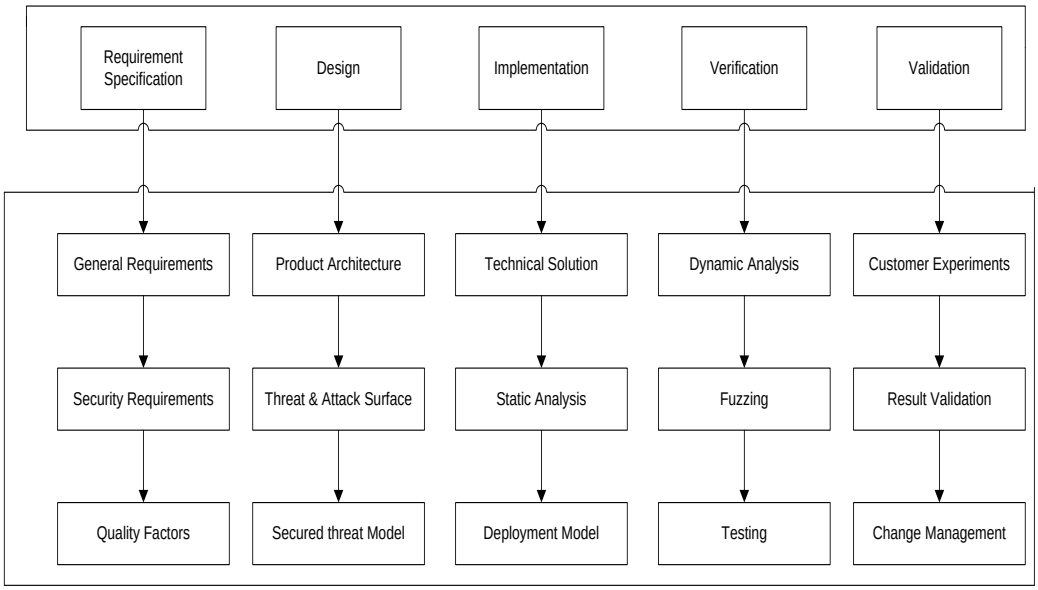

Figure 1. Proposed Secured Software Development Life Cycle Model

Security requirements and analyzed and specified in the first phase of proposed model framework. All the identified requirements with customer feedbacks are included and detailed documentation for specification is developed. Quality factors with each of the identified security and privacy requirements are attached with specification to enhance the focus of the overall quality of the final product.

The design is started from the specification as input under the project and threat attack surface analysis and required privacy factors are derived. All the existing attacks and risks associated with vulnerabilities are modeled with the best suitable solution [7]. Adversarial attacks and their solutions are also included with the design model of the product system which is desired by the customer of the cloud services.

Implementation is started after the successful design. The design model is taken input for the implementation phase and coding is performed to develop the software programs and modules as per specified requirements. Static analysis of the codes are also taken out unit wise to ascertain the overall quality of the codes for secured deployment of the product for customer.

Verification process is after completion of the coding process. A extensive testing procedures are executed with the code and units to find out the gaps between the current outcomes and specified outcome of the product. Fuzzing tools, Structural and functional testing tools are used to test and verify the current developed product with the required specification. All the gaps and identified bugs are removed first to

complete the verification. The testing is performed on the motive to find out and discover the errors in the codes of units, loop homes of the security of cloud-based system product.

At last, the end user or customers are called to validate the final developed product with their own input. The validation process completes when customer gets satisfaction with its input to the current developed product.

The security and privacy requirements are proposed with the methodological way under the requirement analysis process presented in figure 1. Further the detailed security and privacy requirement modeling for the model framework of cloud security by customer viewpoint is elaborated in figure 2.

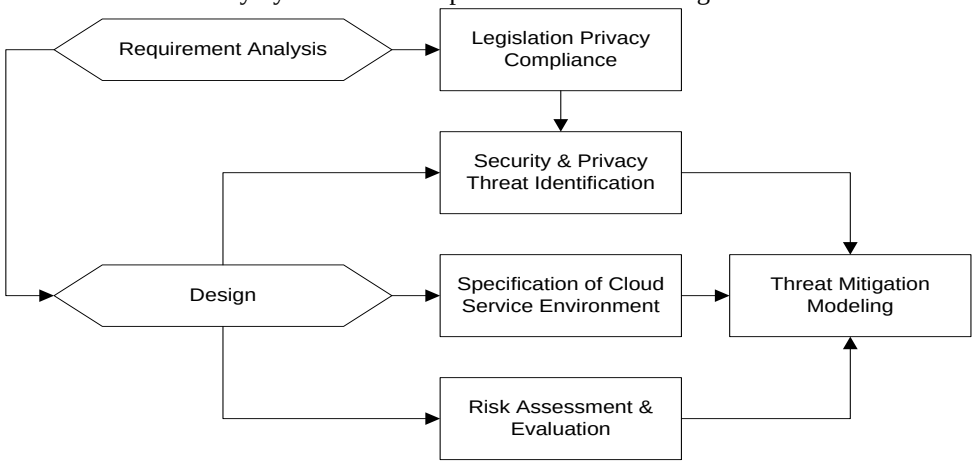

Figure 2. Security and Privacy Model Framework Steps

Our proposed Security and privacy methodology model framework part presented in figure 2. Entails the loop based analysis and specification. This indulges all the stakeholders such as customer users, developers, and other users to input the requirement while analysis process is going on to specify the requirement of the final secured customer specific product of cloud environment [8].

5. Enforcement and Inclusion of Regulation Compliant of Privacy

Adding the privacy regulatory compliant is with software is very difficult in general consideration. This is due to fact that it requires the regional regulatory requirements and their inclusion under the software system. Therefore, customer specific privacy should be in place with respect to the customer region of the operation with the product software. We include a template-basedaspect-oriented scenario to get the privacy requirement details by the customers. This focuses on the specific privacy with given regional privacy requirement to interpret the privacy requirements of customer with its own reginal regulatory requirements [9]. The template for gathering the regional regulatory requirement with respect to customer specific region to include while developing the secured software having specific privacy preserving model framework for cloud software is presented in table 1.

Table 1. Example of customer specific regulatory privacy requirement

Privacy Terms/	**Regulatory Requirement Scope**	**Sensitivity Level**	**Details**
Data Privacy	Sensitive and Critical Data	Very High	Scope defines the specify the business sensitive and critical data privacy
Device Privacy	Network and Computing Devices	Medium	The network devices, servers and other computing workstations
User Privacy	Personal Information	Very High	User personal information should be hidden
Process Privacy	Financial Process Only	High	Process involved in financial transactions should be private between entities
Business Privacy	Sensitive Business Assets	High	Assets which are private to business of organization need privacy
Transformation Privacy	Sensitive Data	Very High	Data transformation for

	Transformation		sensitive data should be private
Processing Privacy	Sensitive Data and shared data	Very High	The share data and sensitive in nature is private among those users only
Transit Privacy	Non Public Data	High	All non public data should be private
Data in Store Privacy	Whole Data	Medium	The data in storage should be hidden to unauthorized access

6. Proposed Cloud Environments

The final cloud software product must have o follow the relevant specified security and regulatory privacy requirement to the customer specific, we proposed the step wise definition of the development process [10]. The process steps are mentioned with following steps.

Step 1. Defining the actors

- Identifying and defining the cloud consumer
- Identifying and defining the cloud provider
- Identifying and defining the cloud broker
- Identifying and defining the user services
- Identifying and defining the cloud carrier

Step 2. Description of the deployment model architecture

- Identification of the cloud components
- Deployment place of the components
- Cloud infrastructure to deploy the components
- Version of the operating system to run cloud software
- Location of the virtual machines
- Location of the database server to run

Step 3. Cloud Service Logical Architecture Model

- Major cloud services specification
- Project requirements and specification for services
- Connectivity and flow of data in virtual environment
- Relationships between the services and defined actors
- Cloud services and their set of properties
- Specific functional requirement with each of the defined cloud services

Step 4. Assets and requirement of Protection

- Defining the assets and their protection need
- Attacker boundaries definition
- Attack vectors and disaster identification

Above four step processes are executed while developing the analysis specification for the project of the cloud software development for specific customer. This framework model provides the high-quality product at the end of the process.

7. Identification of the Privacy Threats

This is additional step wise process which we have included in the analysis process to identify all the privacy threats as per the regulatory requirement of customer specific. The details of each of the steps of this identification of privacy threat in the model framework are step wise evaluation.

Step 1. Selection of the primary needs the specified threat model from previous stages

Step 2. Actors and their role identification

- Selection of the actor role as defined by customer specific requirement of privacy regulatory law
- Roles of cloud data controller
- Roles of data consumer

- Role of cloud controller
- Role of the data processor in cloud environment

Step 3. Defining technical threats by identification
- Finding out the adversaries which violates the privacy
- All identified threats by adversaries are numbered
- Priority to the threats of privacy by adversaries is defined
- Finally model of security and privacy framework is updated

Step 4. Follow the above three steps till all privacy requirements are not served.

8. Evaluating the Risks of Cloud Environment

Risk evaluation is core requirement to provide the secure model framework of the cloud software of the customer. All the risks and associated vulnerabilities are ranked as per the defined priority [11]. We propose the risk variables and threat variables to evaluate the risks.
Risk Variable Vi (V1, V2, V3, … Vn)
Threat Variables Ti (T1, T2, T3,… Tn)

On the basis of defined variables for risks and threats the evaluation of risks is performed. The evaluation matrix is presented in table 2.

Table 2. Risk Factors and Evaluation

Risk Variable	**Name**	**Exploit Scenario**	**Likelihood**	**Severity**	**Users**
T1	Data Accumulation Over time	Huge data is stored from customer side to cloud with respect to the time. It may cause to disclose data	High	Medium	Users of Customer sites, Service provider Side, Third Party
T2	Record linking	Records can be linked by adversarial background Information which leads the leak of data	High	High	Users of Customer sites, Third Party
T3	Data Processes and Cross Linking	Customer can execute the cross linking which leads the hijacking	Medium	High	Users from Customer site, Service Provider site
Tn	As so on	As so on	As so on	As so on	As so on

9. Risk and Threat Mitigation

The security framework model includes the threat mitigation and counter measures are performed. The counter measure for each of the risks identified is defined with respect to the highest likelihood and high level of severity of the risk on prioritized basis [12] [13]. The solution to reduce the risks likelihood is proposed and recommended all the counter measures.

At last stage, the coding is taken to the software system of cloud as per the customer specification and implemented. The effectiveness of the implemented software is tested thoroughly by applying the various testing procedures and methodologies.

10. Future Scope

This paper basically proposes a model of the security framework for the cloud software as per the user specification for the security and privacy as per the regulation requirements proposed the customers. This includes all the artifacts of software development for customer centric software for the cloud application

having the risk and threat evaluation with respect to the customer demands. The scope to enhance this proposed security model framework for customers to include the networksecurity methodologies with adding a specific protocol layer for the specific customer that demands the optimum security framework for their rented cloud solution.

References

[1] F. Swiderski and W. Snyder, Threat Modeling. Redmond, WA, USA: Microsoft Press, 2004.

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing." http://www.csrc.nist.gov/groups /SNS/cloud-computing/, July 2009.

[3] D. Bernstein, "Containers and cloud: From lxc to docker to kubernetes," Cloud Computing, IEEE, vol. 1, pp. 81–84, Sept 2014.

[4] J. Dean and S. Ghemawat, "Mapreduce: A flexible data processing tool," Commun. ACM, vol. 53, pp. 72–77, Jan. 2010.

[5] J. Ralyté, R. Deneckère, and C. Rolland, "Towards a generic model for situational method engineering," in Advanced Information Systems Engineering", vol. 2681 of Lecture Notes in Computer Science, pp. 95–110, Springer Berlin Heidelberg, 2003.

[6] V. Rahimian and R. Ramsin, "Designing an agile methodology for mobile software development: A hybrid method engineering approach," in Research Challenges in Information Science, 2008. RCIS 2008. Second International Conference on, pp. 337–342, June 2008.

[7] A. Gholami and E. Laure, "Advanced cloud privacy threat modeling," Jan Zizka et al. (Eds): CCSIT, SIPP, AISC, CMCA, SEAS, CSITEC, DaKM, PDCTA, NeCoM, p. 229–239, 2016.

[8] A. Gholami, A.-S. Lind, J. Reiche, J.-E. Litton, A. Edlund, and E. Laure, "Design and implementation of the advanced cloud privacy threat modeling," International Journal of Network Security & Its Applications (IJNSA), 2016.

[9] A. Gholami, E. Laure, P. Somogyi, O. Spjuth, NiaziSalman, and J. Dowling, "Privacy-preservation for publishing sample availability data with personal identifiers," Journal of Medical and Bioengineering, vol. 4-2, pp. 117–125, April 2014.

[10] M. Himmel and F. Grossman, "Security on distributed systems: Cloud security versus traditional it," IBM Journal of Research and Development, vol. 58, pp. 3:1–3:13, Jan 2014.

[11] E. Carlini, M. Coppola, P. Dazzi, L. Ricci, and G. Righetti, "Cloud federationsin contrail," in Euro-Par 2011: Parallel Processing Workshops (M. Alexander,P. D'Ambra, A. Belloum, G. Bosilca, M. Cannataro, M. Danelutto, B. Di Martino, M. Gerndt, E. Jeannot, R. Namyst, J. Roman, S. Scott, J. Traff, G. Vallée, and J. Weidendorfer, eds.), vol. 7155 of Lecture Notes in Computer Science, pp. 159–168, Springer Berlin Heidelberg, 2012.

[12] S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and Security for Cloud Computing (S. Pearson and G. Yee, eds.), Computer Communications and Networks, pp. 3–42, Springer London, 2013.

[13] A. Cavoukian, "The Security-Privacy Paradox: Issues, misconceptions, and Strategies." https://www.ipc.on.ca/images/Resources/sec-priv.pdf, 2003. Accessed November 2015.