International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 6 Issue 10|| October 2017 || PP. 33-38

Identification of a new method for modeling threats to privacy in Cloud environments for ensuring privacy requirements in accordance with data protection legislation

Prof.Dr.G.Manoj Someswar[1], K.Madhavi Latha[2]
[1.] *Visiting Professor & Research Supervisor, VBS Purvanchal University, Jaunpur, U.P., India*
[2]. *Research Scholar, VBS Purvanchal University, Jaunpur, U.P., India*

Abstract: *Cloud computing others the prospect of on-demand, elastic computing, provided as a utility service, and it is revolutionizing many domains of computing. Compared with earlier methods of processing data, cloud computing environments provide significant benefits, such as the availability of auto-mated tools to assemble, connect, configure and reconfigure virtualized re-sources on demand. These make it much easier to meet organizational goals as organizations can easily deploy cloud services. However, the shift in paradigm that accompanies the adoption of cloud computing is increasingly giving rise to security and privacy considerations relating to facets of cloud computing such as multi-tenancy, trust, loss of control and accountability. Consequently, cloud platforms that handle sensitive information are required to deploy technical measures and organizational safeguards to avoid data protection break-downs that might result in enormous and costly damages. Sensitive information in the context of cloud computing encompasses data from a wide range of different areas and domains. Data concerning health is a typical example of the type of sensitive information handled in cloud computing environments, and it is obvious that most individuals will want information related to their health to be secure. Hence, with the growth of cloud computing in recent times, privacy and data protection requirements have been evolving to protect individuals against surveillance and data disclosure. Some examples of such protective legislation are the EU Data Protection Directive (DPD) and the US Health Insurance Portability and Accountability Act (HIPAA), both of which demand privacy preservation for handling personally identifiable information.*

There have been great efforts to employ a wide range of mechanisms to enhance the privacy of data and to make cloud platforms more secure. Techniques that have been used include: encryption, trusted platform module, secure multi-party computing, homomorphic encryption, anonymization, container and sandboxing technologies. However, it is still an open problem about how to correctly build usable privacy-preserving cloud systems to handle sensitive data securely due to two research challenges. First, existing privacy and data protection legislation demand strong security, transparency and audibility of data usage. Second, lack of familiarity with a broad range of emerging or existing security solutions to build efficient cloud systems. This dissertation focuses on the design and development of several systems and methodologies for handling sensitive data appropriately in cloud computing environments.

The key idea behind the proposed solutions is en-forcing the privacy requirements mandated by existing legislation that aims to protect the privacy of individuals in cloud-computing platforms. We begin with an overview of the main concepts from cloud computing, followed by identifying the problems that need to be solved for secure data management in cloud environments. It then continues with a description of background material in addition to reviewing existing security and privacy solutions that are being used in the area of cloud computing. Our first main contribution is a new method for modelling threats to privacy in cloud environments which can be used to identify privacy requirements in accordance with data protection legislation. This method is then used to propose a framework that meets the privacy requirements for handling data in the area of genomics. That is, health data concerning the genome (DNA) of individuals. Our second contribution is a system for preserving privacy when publishing sample availability data. This system is noteworthy because it is capable of cross-linking over multiple datasets. This research work continues by proposing a system called ScaBIA for privacy-preserving brain image analysis in the cloud. The final section of the research work describes a new approach for quantifying and minimizing the risk of operating system kernel exploitation, in addition to the development of a system call interposition reference monitor for Lind - a dual sandbox.

Keywords: *Cloud Privacy Threat Modelling (CPTM), Secure Development Life Cycle (SDLC), Threat Modeling Methodology(TMM), pay-as-you-go models.*

Date of Submission: 06-10-2017 Date of acceptance: 18-10-2017

I. Introduction

Danger displaying is an imperative piece of the way toward creating secure programming - it gives an organized approach that can be utilized to distinguish assaults and to propose countermeasures to keep vulnerabilities in a framework from being abused.

As depicted before, the issues of security and protection are truly two particular points [1] as security is a center security idea, and the present concentration of the current risk displaying systems is not on security in distributed computing, which makes it difficult to apply these philosophies to creating security saving programming with regards to distributed computing situations.

We present a cloud security danger displaying procedure as per the standards of ME. The technique that has been connected is one known as "Expansion based", which is utilized for improving the way toward recognizing protection dangers by applying meta-models/designs and predefined necessities. This new approach is being proposed gives solid methodological help to protection enactment and direction in distributed computing situations. We portray a best down way to deal with recognize the necessities for a perfect protection danger displaying technique in distributed computing and fabricate another system by applying the prerequisites that were distinguished.

Whatever remains of this section is composed as takes after. Area portrays the attributes that are attractive in protection danger demonstrating for distributed computing conditions. the depicts the means and items for the proposed new technique. A bridges the conclusions from this examination.

Characteristics of a Privacy Threat Modeling Methodology for Cloud Computing

This area depicts the components that we trust a security danger model ought to have so as to be utilized for creating protection saving programming in mists in an efficient way. In light of the properties that are distinguished, we at that point apply the Extension-based philosophy configuration way to deal with developing an expansion of the CPTM for supporting different security enactment.

Privacy Legislation Support

Methodological help for the administrative systems that characterize security requirements for preparing individual or delicate information is a key concern. Protection enactment and directions can wind up noticeably muddled for cloud clients and programming designing groups, especially as a result of the distinctive phrasings being used in the IT and lawful fields. What's more, security danger displaying are not underlined in existing risk demonstrating procedures, which causes uncertainty for protection risk recognizable proof.

Technical Deployment and Service Models

Distributed computing conveys processing programming, stages, and frameworks as administrations in view of pay-as-you-go models. Cloud benefit models can be conveyed for on-request stockpiling and processing power SaaS, PaaS and IaaS. As depicted before, cloud administrations can be conveyed to purchasers utilizing different cloud sediment models: private cloud, group cloud, open cloud, and half and half cloud.

Customer Needs

The genuine needs of the cloud customers must be thought about all through the entire life-cycle of a venture. Furthermore, over the span of a venture, demands for changes frequently emerge and these may influence the plan of the last framework. Thusly, it is critical to distinguish any protection dangers emerging from the client needs that outcome from such change demands. Consumer loyalty can be accomplished through connecting with clients from the early phases of risk displaying so the subsequent framework fulfils the client's needs while keeping up satisfactory levels of security.

Usability

Cloud-based devices go for diminishing IT expenses and supporting speedier discharge cycles of brilliant programming. Danger displaying instruments for cloud conditions should, consequently, be perfect with the normal quick pace of programming advancement in mists based activities. However creating simple to-utilize items with a proper harmony between keeping up the required levels of protection while fulfilling the buyer's requests can be testing with regards to cloud conditions.

Traceability

Every potential risk that is distinguished ought to be recorded precisely and be traceable in conjunction with the related protection necessities.[2] In the event that dangers can be followed in this way, it implies that risk demonstrating exercises are efficient in the following of the first protection necessities that are incorporated into the logical data and changes over the post prerequisite strides, for example, outline, implementation, check, and approval.

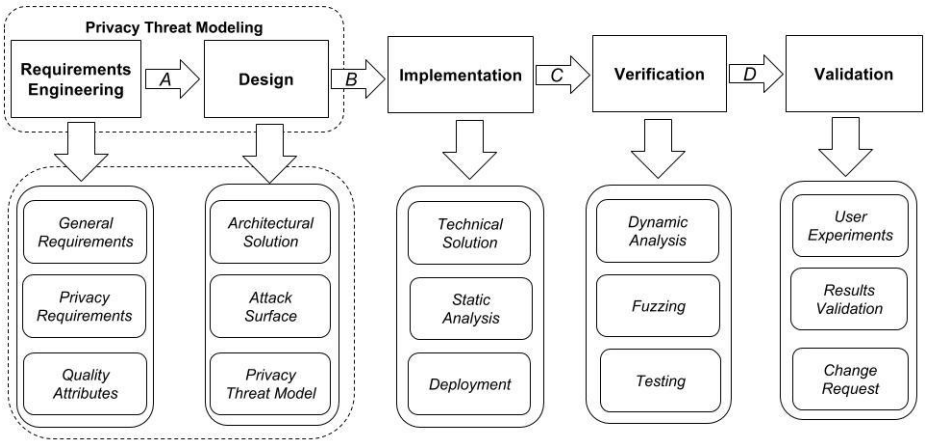
II. Methodology Steps and Their Products

Propelled by the realities that protection and security are two unmistakable themes and that no single philosophy could fit all conceivable programming improvement exercises, we apply ME that intends to develop techniques to fulfil the requests of particular associations or undertakings. In ME is characterized as "the building order to configuration, build, and adjust strategies, procedures, and instruments for the improvement of data frameworks".

There are a few ways to deal with ME, for example, an in a general sense "impromptu" approach where another technique is developed sans preparation, "worldview based" methodologies where a current meta-show is instantiated, preoccupied or adjusted to accomplish the objective strategy, "Expansion based" methodologies that mean to improve a current philosophy with new ideas and components, and "get together based" methodologies where a system is built by gathering technique parts inside a storehouse.

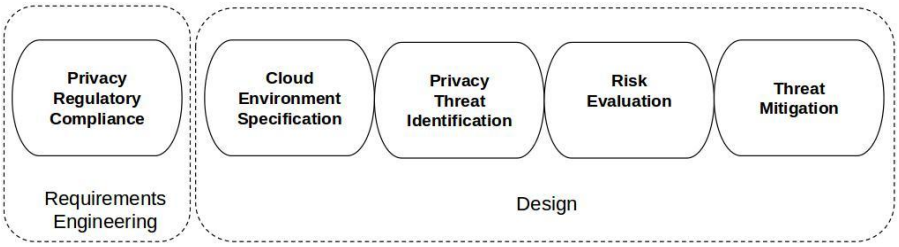
Figure 1 speaks to various stages in a typical Secure Development Life Cycle (SDLC). Starting security prerequisites are gathered and overseen in the requirements building stage (A). This incorporates distinguishing the quality characteristics of the venture and evaluating the hazard related with accomplishing them. An outline is made out of the engineering arrangement, assault surface examination, and the security risk show. Potential protection dangers against the product that is being created are distinguished and arrangements are proposed to relieve for ill-disposed attacks(B). The proposed arrangement from the plan stage is actualized through a specialized arrangement and organization (C). This incorporates performing static examination on the source code for programming understanding without really executing programs. The confirmation procedure (D) incorporates broad testing, dynamic examination on the executing programs on virtual assets and fluffing as a discovery testing way to deal with find coding mistakes and security provisos in the cloud framework. At last, in the Validation stage, the end-clients take an interest to evaluate the genuine outcomes versus their desires, and may advance further change demand.

Figure 1: Privacy threat modelling in requirements engineering and design of a SDLC



Our proposed system distinguishes the protection prerequisites in the Requirements Engineering venture, as appeared in Figure 2. The outcomes from the Requirements Engineering, which incorporate determinations for protection administrative consistence, are sustained into the Design step, where exercises, for example, indicating the suitable cloud environment, recognizing security dangers, assessing dangers and moderating dangers are directed. At that point the delivered security risk model would be utilized as a part of the implementation step at long last it would be confirmed and approved in the resulting steps.

Figure 2: The CPTM methodology step



Cloud partners and members, for example, cloud clients, programming building group and legitimate specialists will participate in the exercises appeared in Figure 2 to actualize the danger display with regards to steps An and B in Figure 1. Cloud programming draftsman as an individual from the product building group starts a learning session to elucidate the procedure steps and their items, protection prerequisites (presenting the law title that is should have been authorized in the cloud condition), and quality traits, for example, execution, ease of use. The lawful specialists will recognize the authoritative necessities that guarantee the protection of information in the stage[3]. In the Design step, the cloud programming planner displays the engineering of the creating cloud condition for different members. This will bring about a bound together phrasing to be utilized as a part of the security risk model. The rest of this segment plots the execution model of the means that are spoken to in Figure 2.[4]

Privacy Regulatory Compliance

Deciphering protection administrative structures can be frequently mind boggling for programming designing groups. In the security administrative consistence step, learning sessions with protection specialists, end-clients and necessities engineers encourages the elicitation of security prerequisites (PR). For instance, in the EU DPD a portion of the protection prerequisites are legality, educated assent, reason authoritative, straightforwardness, information minimization, information exactness, information security, and responsibility. Each of the necessities that are recognized will be marked with an identifier, e.g., (PRi), name and portrayal to be utilized as a part of later stages.

Cloud Environment Specification

To guarantee that the last cloud programming will conform to the important lawful and administrative system, a few of the key qualities that are influenced by distributed computing administrations (counting virtualization, outsourcing, off-shoring, and autonomic advancements) must be indicated. For this reason, the physical/intelligent structures of the arrangement and administration model can be created by the accompanying strides.

Step A: Define the cloud performing artists, (for example, Cloud Consumer, Cloud Provider, Cloud Auditor, Cloud Broker, and Cloud Carrier) [5]. Cloud customer is a man or association utilizes benefit from cloud suppliers with regards to a business relationship. Cloud supplier makes benefit accessible to intrigued clients. Cloud reviewer directs an autonomous appraisal of cloud administrations, operations, execution and security of the organization. Cloud representative deals with the utilization, execution and conveyance of cloud benefits and sets up connections between cloud suppliers and cloud purchasers. Cloud transporter gives availability and transport of cloud administrations from cloud suppliers to cloud customers through the system
Step B: Describe a nitty gritty model of the cloud sending physical architecture where the segments will be sent over the cloud foundation. This should give points of interest of where the segments will be sent and keep running, for instance, the working framework form,[6] the database form, the virtual machine area, and where the database server will run

Step C: Describe the intelligent design of the cloud administrations display where the significant cloud administrations, alongside and the connections between them that are important to satisfy the venture necessities, are recorded.[7] This ought to incorporate the information stream and associations between the significant cloud administrations and on-screen characters. Note that in this unique circumstance, a substance is a cloud benefit with an arrangement of properties that meet a particular utilitarian necessity.

Step D: Describe the benefits that should be secured, the limits of the cloud and any potential aggressors that may jeopardize either the cloud condition or the advantages that have been distinguished as being related with that specific cloud.

The cloud condition detail step comprises of forming a compositional report including resources that are liable to security assurance, cloud performing artists, physical engineering of the arrangement show, and sensible design of the administration display.

Privacy Threat Identification

In this progression, security dangers against the PRs that were built up in protection regulatory consistence definition stage will be distinguished and dissected. To accomplish this, the framework creators will attempt the accompanying strides.

Step A: Select a protection prerequisite from the PR list for danger investigation, e.g., (PR2).

Step B: Correlate recognized cloud performing artists with the performer parts that are characterized in the venture's security law. For instance, correlating the Data Controller part as a Cloud Consumer, or the Data Processor part as a Cloud Provider in the DPD.

Step C: Identify all the specialized dangers that can be propelled by an advertisement adversary to protection and mark them in the predefined cloud condition. Each distinguished risk can be named as a Ti.j, where i shows

that danger T that relates to PRi and j demonstrates the genuine danger number. For instance, in T2.5, digit 2 demonstrates the pertinence of the risk to PR2 and digit 5 is the genuine danger number.
Step D: Repeat the past strides until the point when all PRs are handled The risk recognizable proof stride comprises of creating an examination report including a rundown of dangers including id, name, date, creator, danger situation for each class of the PRs.[8]

Risk Evaluation

In this progression, all on-screen characters take an interest to rank the dangers that have been recognized in past stride as to their evaluated level of significance and the normal seriousness of their effect on the general security of the cloud condition.[9] The Importance shows the probability of a specific danger happening and the level of the Effect demonstrates the reasonable seriousness of the harm if that risk against the cloud condition were done. Expect there are three distinguished PRs (PR1, PR2, PR3) notwithstanding related protection dangers T1.4, T2.1, and T3.3 from past strides for a fanciful cloud sys-tem.[10] In this envisioned cloud, different members in the venture, for example, Alice (Cloud Consumer), Bob (Cloud Provider), Dennis (Software Architect), Tom (Lawyer) and Rosa (Cloud Carrier) assess the relating danger of each distinguished dangers, as outlined in Table 1.

ID	Name	Exploit Scenario	I	E	Participants
T1.4	Data Accumulation over Time	The cloud system stores a huge amount of data from Cloud Consumers over the time. This can be done through extensive analysis of collected data from different sources.	H	M	Alice, Bob, Dennis, Tom
T2.1	Linkability of Records	A record owner can be linked through the adversarial background knowledge for the published data to the Cloud Provider.	H	H	Alice, Bob, Dennis, Tom
T1.4	Cross-linking of data processing	A Cloud Consumer is able to run cross-linking queries over multiple data sets from different data sources.	M	H	Alice, Bob, Dennis, Tom

Table 1: Prioritization of the identified threats, L (Low), M (Moderate), H(High)

Threat Mitigation

In this progression, the risk demonstrating group proposes countermeasures to the dangers that were distinguished in the past stride as having the most noteworthy probability of event and the most noticeably awful potential effects on the cloud condition. Every countermeasure ought to obviously portray an answer that lessens the likelihood of the risk happening and that additionally decreases the negative impacts of the cloud if the danger was done.

At last, the prescribed countermeasures from this progression ought to be recorded and sustained into the execution venture to be acknowledged through coding and for their effectiveness to be evaluated by static investigation. In the later phases of check and approval, each such countermeasure will be assessed and affirmed by the members.

III. Results & Conclusion

In this research paper, we distinguished the prerequisites to manufacture a security risk displaying approach for distributed computing situations utilizing an Extension-based ME approach. For this reason, we presented Cloud Privacy Threat Modelling (CPTM) for consistence with different legitimate and administrative systems, notwithstanding in-demonstrating the danger recognizable proof process.

As verification of idea, we will apply the proposed technique inside the Bio Bank Cloud that expects to prepare the delicate information, as examined in next. This will be an initial step to approve our proposed approach for giving tweaked protection danger demonstrating in bioinformatics distributed computing conditions.

References

[1] D. Bernstein, "Containers and cloud: From lxc to docker to kubernetes," *Cloud Computing, IEEE*, vol. 1, pp. 81–84, Sept 2014."FreeBSD Jails." https://wiki.freebsd.org/Jails. Accessed September 2015.

[2] R. Pike, D. Presotto, K. Thompson, H. Trickey, and P. Winterbottom, "The use of name spaces in plan 9," *SIGOPS Oper. Syst. Rev.*, vol. 27, pp. 72–76, Apr. 1993.

[3] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm." RFC 4226 (Informa-tional), Dec. 2005.

[4] D. M'Raihi, S. Machani, M. Pei, and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm." RFC 6238 (Informational), May 2011.

[5] L. Sweeney, "k-anonymity: a model for protecting privacy," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, pp. 557–570, Oct. 2002.

[6] G. on Statistical Disclosure Control, "Quasi Identififer." http://stats.oecd. org/glossary/detail.asp?ID=6961. Accessed January 2013.

[7] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10,571–588, Oct. 2002.

[8] P. Samarati and L. Sweeney, "Generalizing data to provide anonymity when disclosing information (abstract)," in *Proceedings of the Seventeenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, PODS '98, (New York, NY, USA), pp. 188–, ACM, 1998.

[9] 58. A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discov. Data*, vol. 1, Mar. 2007.

[10] C. L. Liu, *Introduction to combinatorial mathematics*. New York, St Louis, San Francisco: McGraw-Hill, 1968.

[11] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, Nov. 1979.

[12] J. Cappos and S. Torres, "PolyPasswordHasher: Protecting Passwords In The Event Of A Password File Disclosure." https://github.com/ PolyPasswordHasher/. Accessed May 2015.

International Journal of Engineering Science Invention (IJESI) is UGC approved Journal with Sl. No. 3822, Journal no. 43302.

Prof.Dr.G.Manoj Someswar. "Identification of a new method for modeling threats to privacy in Cloud environments for ensuring privacy requirements in accordance with data protection legislation." International Journal of Engineering Research and Applications (IJERA) , vol. 6, no. 10, 2017, pp. 33–38.