ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Trust Score Based TPA in Cloud with Security Standards Prediction and MyPocket Key Store

K.Shirisha Reddy[1], Dr. M.B.Raju[2]

Research Scholar, Dept. of CSE., JNTUH, Hyderabad, India[1]

Doctorate in Computer Science & Engineering, JNTUH, Hyderabad, India[2]

ABSTRACT: Due to the nature of cloud advantages, it is attacking more organizations to use [7]. Organizations storing sensitive data in cloud data storage of different CSP. Major issue is data protection in-terms of accessibility, privacy. Due to lack of technical knowledge from organizations side, data owners are depending on TPA, where TPA to be trustable auditing tool with privacy facility, assessment nature and trust on it. Many more systems are available with different TPA functionality, which are focusing on data privacy, accessibility without having local copy of data at TPA end. But it is also very important to focusing on trust on TPA, which affects for long relational agreements between data owner and Auditor. It TPA is able to predict security standards to incur to protect data then novice cloud data owners can has hassle free about data. Here in this proposed system a new mechanism is defining by considering trust score based TPA with prediction ability to suggest security standards where data owners has fully controlling on their keys with flexible key store named as MyPocket Key Store..

KEYWORDS: cloud security, TPA trust score, risk prediction, cloud audit

I. Introduction

The word “Cloud Computing” is buzzing in IT industry due its huge advantages. Cloud is attracting organizations of different domains like retails, banking, ERP applications, educational and government sectors etc... Different sizes of organizations are also using Cloud environment to host, share data in different mediums. Reasons to get amazing response to cloud structures are many like its scalability in configuration size, its easiness, its inexpensive payment modal, where some Cloud Service Providers (like AWS, Jelastic, Heroku) offereing Pay per usage, hourly and monthly payments. At the same time cloud data storage struggling with security issues, where data owners needs to depend on some out sourcing agents.

A. *Key Participants in Cloud Environment:*

Major key role participants in cloud environment are three , where CSP (Cloud Service Providers) treated as cloud hosting provider who set up all requirements like Hardware’s , Platform tools (like OS virtual images), second participant called as Cloud Subscriber or tenant who hosted their code or data, third participant is end user who access application and data on behalf of tenant.

CSP manage storage setup warehouse of cloud to hold data as persistent mode and non persistent mode. Storage setup must be attack free environment to keep cloud users data. Everything that the application knows and the capacities that could be given by administration are conceivable through storage. The storage holds appropriate information and data on capacity on how they will be executed. Improvement on storage depends on how the storage office shielded from various assaults and accessibility of go down. Could computing is constantly about consistency and accessibility of administration which will actually require the storage to be accessible constantly.

Each capacity, administration and the capacity of storage to give the required information is just conceivable through enhanced infrastructure. This could be considered as the stage behind the storage as the infrastructure

DOI: 10.15680/IJIRCCE.2016. 0406143

helps the storage manage load issues. The infrastructure is a stage wherein it weights the capacity of the storage against the quantity of solicitations. The infrastructure can roll out a few improvements by burden adjusting and even administration.

Data owners has to depends on third party auditors to perform some security operations like authenticating users to access data, monitoring data inflow and outflow between data warehouse and outsourcing. So security auditing places major role to provide data accessibility in eagle eye monitoring modal.

B. *Types of security audits:*

There are two types of audits which are called as Traditional IT audit and Cloud Audit. Traditional IT audits commonly fall into two principle classifications: inside and outside. Inward audits allude to work done by an association's own particular representatives, concern certain hierarchical procedures, and concentrate basically on enhancement and danger administration. Outer audits give an outside point of view on an association's capacity to meet the necessities of different laws and regulations. Associations have utilized traditional IT audits to assess issues, for example, accessibility to approved clients and uprightness and privacy in information storage and transmission.

Be that as it may, what happens when an association's IT assets are moved to the cloud? Since cloud computing takes into account numerous clients over a vast space, it uncovered novel security issues, for example, cloud-particular classification concerns. These dangers posture new difficulties for security examining, however cloud supporters are reacting to them. For example, gatherings, for example, Cloud Security Alliance (CSA) are encouraging institutionalization of cloud secrecy, respectability, and accessibility evaluating.

C. *Security audits goals:*

A traditional IT security review is an examination of an IT gathering's checks, adjusts, and controls. Reviewers count, assess, and test an association's frameworks, practices, and operations to figure out if the frameworks protect the data resources, keep up information uprightness, and work effectively to accomplish the association's business objectives or goals. To support these destinations, IT security reviewers need information from both inner and outside sources [6].

Likewise, cloud computing accompanies its own arrangement of security difficulties. A cloud infrastructure is the aftereffect of a steady three-path arrangement among administration associations, cloud administration suppliers (CSPs), and end clients to guarantee efficiency while keeping up a sensible level of security [6]. A CSP ought to keep information safe from security dangers but then give customers get to anyplace with Internet administration. Moreover, the customer association must check that the cloud computing venture adds to its business objectives, targets, and future needs. Although both ordinary IT security examining and cloud security evaluating offer numerous worries, a cloud security review must address one of a kind issues commonly not took care of in traditional IT security audits [6]. By meetings, the most prompt and clear test lies in reviewers securing adequate learning of cloud computing. Powerful cloud security evaluators must be acquainted with cloud computing wording and have a working learning of a cloud framework's constitution and conveyance strategy [6]. This information guarantees inspectors pay consideration on security figures that may be more critical in cloud security reviewing forms, including straightforwardness; encryption; collocation; and scale, degree, and many-sided quality [6].

II. Related work

Many researched made related to privacy of the data from TPA. Here following are existing approaches focusing on data security and privacy from TPA.

DOI: 10.15680/IJIRCCE.2016. 0406143

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A. *Provable Data Possession at Untrusted Stores [1]:*

This paper introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it [1]. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs [1]. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication [1]. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems [1].

B. *PORs: Proofs of Retrievability for Large Files [2]:*

A POR may be viewed as a kind of cryptographic proof of knowledge (POK), but one specially designed to handle a large file (or bitstring) F [2]. We explore POR protocols here in which the communication costs, number of memory accesses for the approver, and storage requirements of the user (verifier) are small parameters essentially independent of the length of F [2]. In addition to proposing new, practical POR constructions, we explore implementation considerations and optimizations that bear on previously explored, related schemes [2]. In a POR, unlike a POK, neither the prover nor the verifier need actually have knowledge of F [2]. PORs give rise to a new and unusual security definition whose formulation is another contribution of our work [2].

C. *Privacy-Preserving Public Auditing for Secure Cloud Storage [3]:*

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources [3]. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free [3]. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, a secure cloud storage system supporting privacy-preserving public auditing has been proposed [3]. It further extend results to enable the TPA to perform audits for multiple users simultaneously and efficiently [3]. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient [3].

D. *Enabling Public Audit ability and Data Dynamics for Storage Security in Cloud Computing [4]:*

This work studies the problem of ensuring the integrity of data storage in Cloud Computing [4]. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud [4]. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing [4]. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only [4]. While prior works on ensuring remote data integrity often lacks the support of either public audit ability or dynamic data operations, this paper achieves both [4].

III. APPLICATIONS TO USE TPA

Cloud computing offers an extensive umbrella of administrations that can be gotten to anyplace. Nonetheless, certain fields of business in various spaces will have different requirements of their own. Information sorts can likewise change among areas, as can the legitimate and administrative prerequisites ordered for keeping that information safe. Thus, a one-sizefits-all review won't not fulfill every one of the necessities that a particular review ought to. Area customized audits are a perfect arrangement [6]. Doctor's facilities, specialists' workplaces, and medicinal pros are starting to utilize different cloud-based programming applications that permit the offering of patient data to other human services experts. The medicinal space holds exceedingly touchy and private data yet should permit access by evaluators, patients, drug stores, and different organizations, for example, clinics.

Banks have a considerable measure of movement identified with clients getting to benefits from different gadgets day and night. Banks must redesign data relentlessly as well as keep this data secure and accessible to all customers who need access. Yet, in spite of the obviously overwhelming assignment of continually upgrading and securing touchy information, banking in the cloud holds awesome potential. Advantages incorporate the sharing of data among banks if a customer has different records and in addition cost decrease. Albeit flawless security is inconceivable, security frameworks must have the capacity to oppose and react to ruptures, particularly when billions of dollars and various bank records are at danger. A major issue moderately huge banking clouds face is guaranteeing that customer data can't be stolen or sold. As we would like to think, the protections should be twofold [6].

IV. Key Challenges in TPA

While security and protection concerns are comparative crosswise over cloud administrations and traditional non-cloud benefits, those worries are enhanced by the presence of outside control over authoritative resources and the potential for bungle of those advantages. Transitioning to open cloud computing includes an exchange of obligation and control to the cloud supplier over data and additionally framework parts that were beforehand under the client's immediate control. Notwithstanding this natural loss of control, the cloud administration client still needs to assume liability for its utilization of cloud computing administrations keeping in mind the end goal to keep up situational mindfulness, measure choices, set needs, and impact changes in security and protection that are to the greatest advantage of the association [5].

A. *Data protection:*

Here, the real concerns are introduction or arrival of delicate data and also the misfortune or inaccessibility of data. It might be troublesome for the cloud administration client (in the part of data controller) to viably check the data taking care of practices of the cloud supplier. This issue is exacerbated in instances of various exchanges of data, (e.g., between combined cloud administrations or where a cloud supplier utilizes subcontractors) [5].

B. *Loss of administration:*

In an open cloud organization, clients surrender control to the cloud supplier over various issues that might influence security. Yet cloud administration assertion may not offer a responsibility to determine such issues with respect to the cloud supplier, along these lines leaving crevices in security barriers [5].

C. *Obligation ambiguity:*

Obligation over parts of security might be part between the supplier and the client, with the potential for imperative parts of the guards to be cleared out unguarded if there is an inability to distribute obligation unmistakably. This split is prone to shift contingent upon the cloud computing model utilized (e.g., IaaS versus SaaS) [5].

D. *Vendor lock-in:*

Reliance on exclusive administrations of a specific cloud administration supplier could lead to the client being fixing to that supplier. The absence of immovability of uses and data crosswise over suppliers represents a danger of data and administration inaccessibility if there should arise an occurrence of an adjustment in suppliers; subsequently it is a critical if some of the time disregarded part of security. Absence of interoperability of interfaces connected with cloud benefits comparably binds the client to a specific supplier furthermore, can make it hard to change to another supplier [5].

V. Issues in Current System

Based on survey in cloud auditing, so many researches has been done on data possession, data integrity, dynamic auditing, user identity privacy and some on multi-cloud auditing. Here TPA acts as an security auditor to assess system utilization from internal sources and external sources. As the nature of inexpensive cloud pricing data owners are interested to use different cloud services to store/ manage their data. In this way to support with security auditing for different clouds data owner has to depend on different TPA Services where excising TPA system is not supporting security auditing in Heterogeneous clouds. At the same time no research is focusing on trustiness of TPA apart from data security. What are the units to trust TPA to handle security auditing of data from data clients. At the same time data owners may not have technical knowledge on security levels and requirements. So it is need a system to predict and suggest security stands for data owners based on requirement.

VI. Trust Score Calculator

Cloud environment needs to support multiple security, privacy and trust requirements where cloud is based on multi-domain environment. To handling security assessment in data , cloud data owners are depending on TPA. TPA acts as a Guard between data and users. But here the major issue is how much trust can place on TPA to be as Auditor for cloud data. Trust score can be calculated based on response time with respect of type of data, size of data, can be calculated based on types of assessments can be handled, can be calculated based on communication or network Overhead can be calculated based on check proof success and failures ratio can be calculated based on metadata correctness.

VII. Simulation Results

In this section, we present the detailed explanation of “Domain Relation Matrix”, which can be represented as DRM in next coming sections. DRM is a dynamic matrix which defines the relation among TPA, CSP and Application Domains. Relation in DRM is a service providing by TPA with respect to CSP.

Let $\mathrm{TPA}_N = \{TPA_1, TPA_2, - - -TPA_N\}$ is a set of registered TPA’s. Where $\mathrm{TPA}_{i,}$ is ith TPA, $i \leq N$.
$\mathrm{CSP}_J = \{CSP_1, CSP_2, - - -CSP_J\}$ is a cumulated set of CSP’s, which are supported by any one of the registered TPA.
$\mathrm{D}_K = \{D_1, D_2, - - -D_K\}$ is a set of domains supported by any one of the registered TPA on behalf of CSP.

We can represent set of available services as S, which defined as bellow

$$(TPA \times CSP \times D\ ) \in \mathbf{S} \quad \text{----------------- Eq (1)}$$

Where S defined as list of available services, means TPA_i is providing service to CSP_j for domain D_k can be represented as $\left(TPA_i \times CSP_j \times D_k\right) \in \mathrm{S}$. DRM contains TPA as columns and supporting CSP’s as first row proceeding by rows which defined list of domains supported by TPA for its supported corresponding CSP. Each element of DRM is a vector, where vector consists CSP’s or domains as elements. Size of DRM is **(J+1) × N,** where J is total CSP’s and N is total TPA’s.

For better understanding of DRM element placement, we consider following situation, where 2nd TPA is supporting service for 1st CSP and for 2nd domain then DRM element is represented as $(TPA_2 \times CSP_1 \times D_2) \in \mathrm{S}$, index of element will be (2, 2) , means $(TPA_2 \times CSP_1 \times D_2) \in \mathrm{S}$ is in second row and second cell, so that $\mathrm{DRM}_{(2,2)} \neq \mathrm{null}$.

TPA's →	TPA1	TPA2	TPA3
CSP Vector	CSP1 CSP2 CSP3	CSP1 CSP3	CSP2 CSP3
CSP1	D1 D4	D1 D2 D3 D4	**Null**
CSP2	D2 D3 D4	**Null**	D1 D2
CSP3	D1 D2 D3 D4	D2 D3	D1 D3 D4

Fig1: DRM

Deep element of DRM includes domain position into element index. In considered DRM example, deep element position of D2 for TPA1 and CSP1 is (2,1,2). Deep Element Value (DEV) defined as

$$DEV_{(n,j,k)} = \begin{cases} 1, & if \;\; \mathrm{DRM}_{(j+1,n)} \neq \text{null} \;\; \textbf{and} \; \mathrm{D}_{k} \in \mathrm{DRM}_{(j+1,n)} \\ 0, & Otherwise \end{cases} \quad \text{----------------- Eq (2)}$$

DEV$_{(n,j,k)}$ is 1 means TPA$_{n}$ is supporting CSP$_{j}$, & is supporting D$_{k}$, DEV$_{(n,j,k)}$ is 0 means D$_{K}$ is not supporting by TPA$_{n}$. DEV is useful to find out whether domain is supporting by TPA and its CSP, or not.

Element Value (EV) is useful to find out whether CSP is supporting by TPA or not. EV can be defined as

$$EV_{(n,j)} = \begin{cases} 1, & if \;\; \mathrm{DRM}_{(j+1,n)} \neq \text{null} \\ 0, & Otherwise \end{cases} \quad \text{------------------- Eq (3)}$$

EV$_{(n,j)}$ is 1 means TPA$_{n}$ is supporting CSP$_{j}$, is 0 means TPA$_{n}$ is not supporting CSP$_{j}$. DEV is useful at the time of Trust Score calculation, when input includes TPA, CSP and Application Domain, EV is useful when input includes TPA and CSP. To calculate Trust Score DEV or EV must be 1 for given input.

VIII. Conclusion

As the nature of cloud, will attract technical and non technical users to use for organizational purpose. No guaranty that every cloud data owner knows about security risk levels and Standards in the field of cloud environment. So our proposed system is very useful for predicting security standards for cloud data owners to make assessment easy. It acts as a filter before performing an testing actions by test user It can create test users with different roles automatically It can perform actions on behalf of created users with roles. It captures actions and used data during test phase Map with security dictionary to predict security standards.

References

1. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., Song, D.: Provable data possession at untrusted stores. Proceedings of the 14th ACM conference on Computer and communications security - CCS '07,2007
2. Juels, A., Kaliski, B.: Pors: proofs of retrievability for large files. Proceedings of the 14th ACM conference on Computer and communications security - CCS '07,2007
3. Wang, C., Chow, S., Wang, Q., Ren, K., Lou, W.: Privacy-Preserving Public Auditing for Secure Cloud Storage. IEEE Transactions on Computers. 62, pp. 362-375 ,2013.
4. Wang, Q., Wang, C., Ren, K., Lou, W., Li, J.: Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. IEEE Trans. Parallel Distrib. Syst. 22, pp. 847-859, 2011.
5. Cloud-council.org,: Cloud Standards Customer Council | CSCC, http://www.cloud-council.org.
6. InfoQ,: Cloud Security Auditing: Challenges and Emerging Approaches, http://www.infoq.com/articles/cloud-security-auditing-challenges-and-emerging-approaches.
7. Mell P, Grance T (2009) A NIST definition of cloud computing. National Institute of Standards and Technology. NIST SP 800-145. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf, 2009.

8. IDC Enterprise Panel, September. http://www.slideshare.net/JorFigOr/cloud-computing-2010-an-idcupdate,2009.
9. Cloud Industry Forum Cloud UK: Adoption and Trends 2011. 4. Cloud Security Alliance (2010) Top Threats to Cloud Computing. v1.0, March, 2011.
10. Horrigan JB , Use of cloud computing applications and services. Pew Internet & American Life project memo, Sept.
11. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) (2001) Title V, pp.505, 2001.
12. Daniele Catteddu and Giles Hogben , ENISA Cloud Computing: Benefits, risks and recommendations for information security, November,2009

BIOGRAPHY

Mrs.K.Shirisha Reddy Ph.D scholar (CSE) from JNTU-H in Cloud Computing. She is working as an Associate Professor in Vignan Bharathi Institute of Technology, Hyderabad, Telangana, India. Her researching areas are heavily focusing on producing best quality cloud mechanisms.

Dr.M.BALARAJU, B.E(E.C.E), M.Tech(CSE), PhD(CSE) and having 21 years of Teaching Experience. He is working as a Principal in KRISHNA MURTHY INSTITUTE OF TECHNOLOGY, Hyderabad, Telangana, India. His Area of interests are Image processing, Web Mining, Text Mining, Big Data.