TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 5
ISSN: 2054 - 7420

Modeling Structural Behaviour of Inhibitors of Cloud Computing: A TISM Approach

[1]Ambikadevi Amma. T, [2]N. Radhika and [3]Pramod V.R.
[1]Karpagam University, Coimbatore, India
[2]Computer Science & Engg Dept, Amrita University, Coimbatore, Tamil Nadu, India
[3]Dept. of Mechanical Engineering, NSS College of Engg, Palakkad, Kerala, India
prof.ambikadevit@gmail.com; n_radhika@cb.amrita.edu; pramodram09@gmail.com

ABSTRACT

Cloud computing is the delivery of computer resources over a network through web browsers, while the actual physical location and organization of the equipment hosting these resources are hidden from the users. Some of the IT organizations are undergoing severe budgetary constraints depends on clouds for the infrastructure and services. The major attributes of cloud computing are multi-tenancy, massive scalability, elasticity, pay as you use and self-provisioning of resources of the cloud. Cloud computing strategy is subjected to many inhibitors. For finding the interrelationship among inhibitors ISM (interpretive structural modeling) is used which a well is proved technology for finding the interrelationship among elements. An innovative version of interpretive structural model is known as Total Interpretive Structural Model (TISM). In Total Interpretive Structural Modeling (TISM), influence/enhancement of inhibitors and their interrelationship is considered. Total interpretive structural model consists of the following steps. They are identification of elements, pair-wise comparison, level partition, interaction formation, diagraph representation and diagrammatic representation of total interpretive structural model. The methodology of TISM is used to delineate the hierarchical relationship of inhibitors of cloud computing.

Keywords: Cloud computing, Inhibitors, Partition levels, Interaction matrix, TISM.

1 Introduction

Cloud computing is enhancing the effectiveness of computer services while operating in the furious industrial environment. Cloud service providers comply with strict operation policies and measurements to minimize failures in the system. The strategies of cloud computing is subjected to many inhibitors. Cloud computing facility is availed by the customers through internet by using any web browsers. Cloud computing services are having many issues. As these issues are broken with innovation, cloud will move from consumers of small medium business to larger and larger enterprise deployments. Top challenges of cloud computing are security, performance, availability and integrity of data. A great deal of uncertainty is pertained about the security at different levels of network. Network security solutions are not in tolerance with the movement required for cloud to deliver its promise and cost efficiencies. A large number of servers may be present in the cloud .The potential to consolidate millions of servers into dynamic meshes is the biggest pay-off cloud computing. Market valuation and growth potential

DOI: 10.14738/tnc.25.390
Publication Date: 23th September 2014
URL: http://dx.doi.org/10.14738/tnc.25.390

depend on the security, physical infrastructure and network management. Privacy is the accountability to data and transparency to an organization practice about personal information existing. Compliance requirements impact in many ways. Cloud can have cross multiple jurisdictions .Data may be stored in different countries or may be in different states.

Cloud Computing is a new scenario in which customers can use the services and infrastructures by paying an amount for their usage. This is beneficial to some of the IT organizations undergoing severe budgetary constraints for the development of infrastructures and enhancement of hardware and software. The core technologies used in cloud are web applications, services, virtualization and cryptography. The services rendered through cloud are Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). In Software as a Service, the service providers provide the users the service of using any type of application software. In IaaS, the service providers provide the networking equipment, storage backups and servers. In PaaS the service providers provides the platform to the users any type of operating systems along with hardware and Software.

Cloud computing is the delivery of computing resources as a service rather than as a product, whereby information is provided to computers and other devices as a utility over a network. Cloud computing describes a new supplement , consumption, and delivery model for IT services based on internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources. Cloud computing providers deliver application via the internet, which are accessed from a web browser.

2 Literature Survey

Cloud computing is becoming a well-known buzz word now a days. Privacy issues and security problems are pointed out as barriers for users to adopt into cloud computing systems. Users of cloud computing worry about their business information and critical IT resources in the cloud computing systems which are vulnerable to be attached [1]. Cloud computing allows providers to develop, deploy and run applications that can easily grow in capacity work rapidly without any concern on the properties and the locations of the undergoing infrastructures [2]. Availability is one of the goals of security. It ensures the user to use them at any time at any place. Hardening and redundancy will enhance the availability of the cloud system. Many cloud computing system provide cloud infrastructure and platforms based on virtual machine [Farzad Sabahi,2011] Confidentiality means keeping user's data secret in the cloud system.

Data integrity means prurience the information. No change or no modification by unauthorized users. Access control is another good in security. Access control means to regulate the use of the system including applications, infrastructure and data. Auditing is another phenomenon that could be added as an additional layer above the virtualized OS hosted on the virtual machine [7].Secret information of individual users and business are stored and managed by the service providers.

Cloud computing raises a range of important policy issues, which include issues of Privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others. Users will expect Reliability and Liability on the cloud service resource. Especially if a cloud provider takes over the task of running "mission-critical" applications and will expect clear delineation of liability if serious problems occur. Users will expect that the cloud provider will prevent unauthorized access to both data and code, and sensitive data will remain private. Users will expect to be able to access and use the cloud where and when they wish without hindrance from the cloud provider or third

parties, while their intellectual property rights are upheld. Each of these interrelated issues will be considered in terms of its importance, what realistic expectations users might have, and the policy implications.

S. Pearson et al describe privacy manager mechanism in which user's data is safe on cloud. In this technique the user's data is in encrypted form. Privacy manager make readable data from result of evaluation manager. In obfuscation data is not present on Service provider's machine so there is no risk with data, so data is safe on cloud but this solution is not suitable for all cloud applications. When input data is high these methods require a large amount of memory [2]. In [3], the authors present procedural and technical solution; both are producing solution to accountability to solve security risk in cloud. Here policies are decided by the parties that use, store or share that data irrespective of the jurisdiction in which information is processed. But it has limitation that data processed on SP is in unencrypted form at the point of processing .So there is a risk of data leakage. In [4], the author gives a language which permits to serve data with policies by agent; agent should provide their action and authorization to use particular data. In this logic data owner attach policies with data, which contain a description of which actions are allowed with each data. In [5], authors give a three layer architecture which protects information leakage from cloud. It provides three layers to protect data. In first layer the service provider should not view confidential data, in second layer service provider should not do the indexing of data, in third layer user specify use of his data and indexing policies. In [6], authors present accountability in federated system to achieve trust management. The trust towards use of resources is accomplished through accountability so to resolve problem for trust management. In federated system they have given three layer architecture, First layer is authentication and authorization. Public key cryptography is used in first layer. Second layer is accountability which perform monitoring and logging. The third layer is anomaly detection which detects misuse of resources. This mechanism requires third party services to observe network resources.

Interpretive structural modeling is a well-established methodology for identifying relationships among elements present in a complex structure [15]. ISM is an interactive learning process in which set of directly or indirectly related elements are structured into a comprehensive model. For identity relationships among items, the ism methodology can be established. The variables in the specific problem or issue are identified first and then a contextually relevant subordinate relation is taken. Based on pair-wise comparison of variables, a structural self-interaction matrix (SSIM) is developed from the element set. Transitivity is checked and a matrix model is obtained. ISM is derived from the partitioning of the element and an extractive of the structural model [10]. In this approach conceptual and computational leverage are exploited to explain the contextual relationship among a set of variables. According to Warfield [11] a set of requirement are needed for interpretive structural modeling. They are: a) Inclusion of scientific elements b) A complex set of relation can be exhibited c) Complex set of relations permits continuous observation, questioning and modification d) Consequence with perceptions and analytical process of the originators e) Public audience can early learn.

3 Methodology

ISM is an interpretive learning process. Judgment of the group decides the relationship of different elements in the system. Over all structure is extracted from the set of elements on the basis of mutual relationship hence it is structural and overall structure is portrayed in a diagraph model hence it is a

modeling technique. Total Interpretive Structural Model has some common steps of ISM. Reachability and partition levels are adopted as it is in the process of interpretive structural model. Steps for obtaining Total Interpretive Structural Model is briefly described below.

3.1 Step I: Inhibitors identification and its definition

First step in any structural modeling is identification and definition of elements whose relationship is to be studied. For these purpose inhibitors of cloud computing is identified from literature survey and discussions with domain experts and is shown in Table1.

Table 1: Inhibitors and definitions.

In. No.	Name of inhibitors	Definition
1	lack of sufficient security	Security in cloud has boarder area comprising software security hardware security
2	Lack of reliability	Data taken from clouds should be correct in all sense. Customer can rely on the service of cloud
3	Lack of portability	It is important to map out the dataflow from the current infrastructure to an eventually cloud service provider whether private or public cloud.
4	Lack of privacy	Privacy is the accountability to data and transparency to an organization. Personal information should be kept constant.
5	Lack of standardization	Standards are scares with in the cloud. Mass adoption is difficult without standards.
6	Lack of comprehensive management tool	These tools would help automatic service provisioning balance workloads and aids with capacity planning and configuration management
7	Week access control	We will have more control to manage and racking of servers, networking and cabling as well as security
8	Lack of data confidentiality	Customers should have fading that every service getting through cloud is correct and secure. Hence confidence on cloud will increase
9	Ineffective backup management	Since everything depend on computation any error can cause defects or destruction .Hence a backup is very necessary and new not available
10	Cost/time barrier	It should be evaluated closely as a cloud migration could actually be much more feasible realistic and less expensive then companies actually realize
11	.Network management barrier	Changes in the security requirement may change the topology of network.
12	Legal issues.	Cloud services may be among countries. .Different countries are having different jurisdiction which may affect cloud services.
13	Infrastructure security at network level	For using public cloud the topology of the network may vary with the security requirement
14	Infrastructure security at host level	Virtualization security threads like VM escape, system configuration drifts and inside threads
15	Infrastructure security at application level	Application security spectrum should be considered web browser security should be taken into account
16	Lack of data integrity	Data should be correct in all means so that integrity validation should be applied
17	Lack of data availability	Customer requirement may be satisfied by making the data in cloud availability to everyone
18	Lack of data security	Data security includes the security of stored data and retrieving data.

3.2 Step II: Contextual relationship definition

Structural Self Interaction matrix is developed by relating elements contextual relationship. Contextual relationship between different inhibitors is studied. Inhibitor 1 is compared with all other inhibitors and study .how inhibitor1 influence/enhance inhibitor 2 and how inhibitors 1 influence/enhance inhibitor 3 etc. To capture the contextual relationship among inhibitors experts opinion is solicited.

3.3 Step III: Interpretation of relationship

In traditional ISM contextual relationship remains silent. Relationship alone is charted out but not given importance on how that relationship really works. In TISM explanation of how the inhibitors influence /enhance with each other is considered. It also explain in what way they influence /enhance each other.

3.4 Step IV: Pair-wise comparison

A pair-wise comparison of elements is used to develop SSIM (Structured Self interaction Matrix.) In formal ISM interpretation indicate direction of relationship only when there is relation among elements. When there is relation from i to j -V, j to i -A, i to j and j to i -X and for no relation O is used. TISM make use of the concept by answering the interpretive query in step III. For each paired comparison, first element should be compared with all the remaining elements .For each comparison the entry should be Y for relation or N for no relation. The reason for Y should be provided. Comparing all the row elements, a paired relationship in the form of interpretive logic –knowledge base is obtained and is shown in Table 2.

Table 2: Interpretive logic –knowledge base

Inhibitor No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
I	Y	Y	N	N	N	N	Y	Y	N	N	Y	N	Y	Y	N	Y	Y	Y
2	N	Y	N	N	Y	N	N	Y	N	N	N	Y	N	N	N	Y	Y	Y
3	N	N	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	Y	Y
4	Y	Y	N	Y	N	N	Y	Y	N	N	N	Y	Y	N	N	Y	Y	Y
5	N	N	N	N	Y	Y	N	Y	N	N	N	Y	N	N	N	N	Y	Y
6	N	Y	N	N	Y	Y	N	Y	N	N	N	Y	N	N	N	Y	Y	Y
7	N	N	Y	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y
8	Y	N	N	Y	Y	N	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y
9	Y	Y	N	N	N	N	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
10	N	N	Y	N	Y	Y	N	N	N	N	N	Y	N	N	Y	Y	Y	Y
11	N	Y	N	N	Y	Y	N	Y	N	N	N	Y	Y	N	N	N	N	N
12	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	Y	Y
13	N	Y	N	N	Y	N	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y
14	N	Y	N	N	Y	N	Y	Y	N	N	N	Y	N	Y	N	Y	Y	Y
15	Y	Y	N	N	Y	N	Y	Y	N	Y	N	N	Y	Y	Y	Y	Y	Y
16	Y	N	N	Y	Y	N	Y	Y	N	Y	N	Y	N	N	N	Y	Y	Y
17	Y	N	N	Y	N	N	Y	Y	N	Y	N	Y	N	N	N	Y	Y	Y
18	Y	N	N	Y	Y	N	Y	Y	N	Y	N	Y	N	N	N	Y	Y	Y

3.5 Step V: Reachability Matrix and Transitivity check.

Y in the knowledge base cell is replaced by 1and N is replaced by 0 in reachability matrix. Check for transitivity and reachability matrix is constructed as shown in Table 3.

Table 3: Reachability matrix

Inhibitor No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
I	1	1	0	0	0	0	1	1	0	0	1	0	1	1	0	1	1	1
2	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	1	1
3	0	0	1	0	0	0	0	1	0	0	1	1	0	0	0	0	1	1
4	1	1	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	1
5	0	0	0	0	1	1	0	1	0	0	1	1	0	0	0	0	1	1
6	0	1	0	0	1	1	0	1	0	0	1	1	0	0	0	1	1	1
7	0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1
8	1	0	0	1	1	1	1	1	0	0	0	1	1	1	1	1	1	1
9	1	1	0	0	0	0	1	1	1	0	1	0	1	1	1	1	1	1
10	0	0	1	0	1	1	0	0	0	1	1	1	0	0	1	1	1	1
11	0	1	0	0	1	1	0	1	0	0	1	1	1	1	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1
13	0	1	0	0	1	0	1	1	0	0	1	1	1	1	1	1	1	1
14	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	1	1	1
15	1	1	0	0	1	0	1	1	0	1	1	0	1	1	1	1	1	1
16	1	0	0	1	1	0	1	1	0	1	0	1	0	0	0	1	1	1
17	1	0	0	1	0	0	1	1	0	1	0	1	0	0	0	1	1	1
18	1	0	0	1	1	0	1	1	0	1	0	1	0	0	0	1	1	1

3.6 Step VI: Level Partition in Reachability Matrix.

ISM based level partition is carried out. Reachability set and antecedent sets for all the elements are determined. Intersection of the two sets is found out. The elements for which the reachability set and intersection set remain same, occupy the top level in ISM hierarchy. Top level elements will not influence the remaining elements hence it can be removed from further calculation. The same process is repeated until the levels of each element are found out. Level partition details are shown in Table 4 to 12.

Table 4 - 1st Level partition

Inhibit No.	Reachability Set	Antecedent Set	Intersection	Level
1	1,2,7,8,11,13,14,16,17,18	1,4,8,9,15,16,17,18	1,8,16,17,18	
2	2,5,8,11,12,16,17,18	2,4,6,9,11,13,14,15	2,11	
3	3,11,12,17,18	3,5,7,10,11	3,11	
4	1,2,4,7,8,11,12,13,14,16,17,18	4,7,8,16,17,18	4,7,8,16,17,18	
5	5,6,8,11,12,17,18	2,5,6,7,8,10,11,13,14,15,16,18	5,6,8,11,18	
6	2,5,6,8,11,12,16,17,18	5,6,7,10,11	5,6,11	
7	3,4,5,6,7,8,11,12,13,14,15,16,17,18	1,4,7,8,9,13,14,15,16,17,18	4,7,8,13,14,15,16,17,18	

8	1,4,5,7,8,12,13,14,15,16,17,18	1,2,4,5,6,7,8,9,11,13,14,15,16,17,18	1,4,5,7,8,13,14,15,16,17,18	
9	1,2,7,8,9,11,13,14,15,16,17,18	9	9	
10	3,5,6,10,11,12,15,16,17,18	10,15,16,17,18	10,15,16,17,18	
11	2,5,6,8,11,12,13,14	1,2,3,4,5,6,7,9,10,11,13,14,15	2,5,6,11,13,14	
12	12,17,18	2,3,4,5,6,7,8,10,11,12,13,14,16,17,18	12,17,18	1
13	2,5,7,8,11,12,13,14,15,16,17,18	1,4,7,8,9,11,13,15	7,8,11,13,15	
14	2,5,7,8,11,12,14,16,17,18	1,4,7,8,9,11,13,14,15	7,8,11,14	
15	1,2,5,7,8,10,11,13,14,15,16,17,18	7,8,9,10,13,15	7,8,10,13,15	
16	1,4,5,7,8,10,12,16,17,18	1,2,4,6,7,8,9,10,13,14,15,16,17,18	1,4,7,8,10,16,17,18	
17	1,4,7,8,10,12,16,17,18	1,2,3,4,5,6,7,8,9,10,12,13,14,15,16,17,18	1,4,7,8,10,12,16,17,18	
18	1,4,5,7,8,10,12,16,17,18	1,2,3,4,5,6,7,8,9,10,12,13,14,15,16,17,18	1,4,5,7,8,10,12,16,17,18	

Table 5-2nd Level

Elements	Reachability Set	Antecedent Set	Intersection	Level
1	1,2,7,8,11,13,14,16	1,4,8,9,15,16	1,8,16	
2	2,5,8,11,16	1,2,4,6,9,11,13,14,15	2,11	
3	3,11	3,5,7,10,11	3,11	2
4	1,2,4,7,8,11,13,14,16	4,7,8,16	4,7,8,16	
5	5,6,8,11	2,5,6,7,8,10,11,13,14,15,16	5,6,8,11	
6	2,5,6,8,11,16	5,6,7,10,11	5,6,11	
7	3,4,5,6,7,8,11,13,14,15,16	1,4,7,8,9,13,14,15,16	4,7,8,13,14,15,16	
8	1,4,5,7,8, 13,14,15,16	1,2,4,5,6,7,8,9,11,13,14,15,16	1,4,5,7,8,13,14,15,16	
9	1,2,7,8,9,11,13,14,15,16	9	9	
10	3,5,6,10,11,15,16	10,15,16	10,15,16	
11	2,5,6,8,11,13,14	1,2,3,4,5,6,7,9,10,11,13,14,15	2,5,6,11,13,14	
13	2,5,7,8,11,13,14,15,16	1,4,7,8,9,11,13,15	7,8,11,13,15	
14	2,5,7,8,11,14,16	1,4,7,8,9,11,13,14,15	7,8,11,14	
15	1,2,5,7,8,10,11,13,14,15,16	7,8,9,10,13,15	7,8,10,13,15	
16	1,4,5,7,8,10,16	1,2,4,6,7,8,9,10,13,14,15,16	1,4,7,8,10,16	

Table 6-3rd Level

Elements	Reachability Set	Antecedent Set	Intersection	Level
1	1,2,7,8, 13,14,16	1,4,8,9,15,16	1,8,16	
2	2,5,8, 16	1,2,4,6,9,13,14,15	2	
4	1,2,4,7,8,13,14,16	4,7,8,16	4,8,16	
5	5,6,8	2,5,6,7,8,10,13,14,15,16	5,6,8	3
6	2,5,6,8, 16	5,6,7,10	5,6	

7	4,5,6,7,8, 13,14,15,16	1, 4,7,8,9,13,14,15,16	4,7,8,13,14,15,16	
8	1,4,5,7,8, 13,14,15,16	1,2,4,5,6,7,8,9,13,14,15,16	1,4,5,7,8,13,14,15,16	
9	1,2,7,8,9, 13,14,15,16	9	9	
10	5,6,10, 15,16	10,15,16	10,15,16	
13	2,5,7,8, 13,14,15,16	1,4,7,8,9,13,15	7,8,13,15	
14	2,5,7,8, 14,16	1,4,7,8,9,13,14,15	7,8,14	
15	1,2,5,7,8,10, 13,14,15,16	7,8,9,10,13,15	7,8,10,13,15	
16	1,4,5,7,8,10,16	1,2,4,6,7,8,9,10,13,14,15,16		

Table 7-4th Level

Elements	Reachability Set	Antecedent Set	Intersection	Level
1	1,2,7, 13,14,16	1,4,9,15,16	1,16	
2	2,16	1,2,4,9,13,14,15	2	4
4	1,2,4,7,13,14,16	4,7,16	4,7,16	
7	4,7,13,14,15,16	1,4,7,9,13,14,15,16	4,7,13,14,15,16	
9	1,2,7, 9, 13,14,15,16	9	9	
10	10, 15,16	10,15,16	10,15,16	
13	2,7,13,14,15,16	1,4,7,9,13,15	7,13,15	
14	2,7,14,16	1,4,7,9,13,14,15	7,14	
15	1,2,7,10, 13,14,15,16	7,9,10,13,15	7,10,13,15	
16	1,4,7, 10,16	1,2,4,7,9,10,13,14,15,16	1,4,7,10,16	

Table 8-5th Level

Elements	Reachability Set	Antecedent Set	Intersection	Level
1	1, 7, 13,14	1,4,9,15	1	
4	1, 4,7,13,14	4,7	4,7	
7	4, 7, 13,14,15	1,4,7,9,13,14,15	4,7,13,14,15	
9	1, 7, 9, 13,14,15	9	9	
10	10, 15	10,15	10,15	
13	7,13,14,15	1,4,7,9,13,15	7,13,15	
14	7,14	1,4,7,13,14,15	7,14	5
15	1,7,10, 13,14,15	7,9,10,13,15	7,10,13,15	

Table 9 -6th Level

Elements	Reachability Set	Antecedent Set	Intersection	Level
1	1,13	1,4,9,15	1	
4	1, 4,13	4	4	
9	1,9, 13,15	9	9	
10	10, 15	10,15	10,15	6
13	13,15	1,4,9,13,15	13,15	
15	1,10, 13,15	9,10,13,15	10,13,15	

Table 10-7th Level

Elements	Reachability Set	Antecedent Set	Intersection	Level
1	1,13	1,4,9	1	
4	1, 4,13	4	4	
9	1,9, 13	9	9	
13	13	1,4,9,13	13	7

Table 11-8th Level

Elements	Reachability Set	Antecedent Set	Intersection	Level
1	1	1,4,9	1	8
4	1, 4	4	4	
9	1,9	9	9	

Table 12.-9th Level

Elements	Reachability Set	Antecedent Set	Intersection	Level
4	4	4	4	9
9	9	9	9	9

3.7 Step VII: Diagraph development.

The elements are arranged graphically in levels and links are drawn as per the relationship. Diagraph is used to represent the elements and their interdependence in terms of nodes and edges. Elements are arranged graphically in levels and the directed links are drawn as per the relationship shown in reachability matrix. Diagraph is shown in Figure 1.

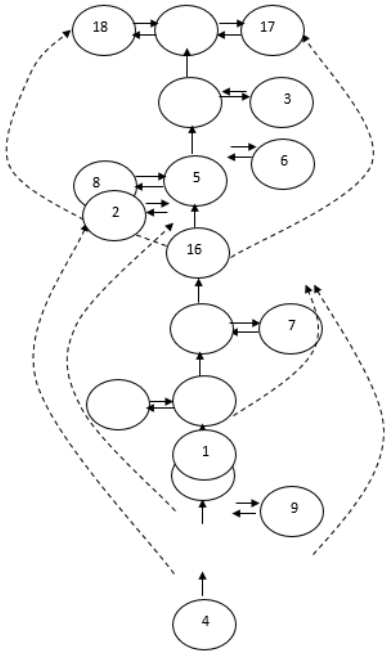

Figure 1: Diagraph with significant transitive links.

3.8 Step VIII: Interaction matrix.

The diagraph is translated into a binary interaction matrix form depicting all the interactions by 1 in cells. Remaining cell entry is 0. Cell with 1 is interpreted by picking the relevant interpretation from the knowledge base in the form of interpretations matrix. Interpretation matrix is shown in

Table 13. Explanation of interpretation matrix is as given below.

Table 13.-Interpretation Matrix.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0
2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
3	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
4	1	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0
5	0	0	0	0	1	1	0	1	0	0	1	0	0	0	0	0	0	0
6	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
8	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0
9	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0
11	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1
13	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0
14	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	0
15	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0
16	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0
17	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0
18	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1

1-13—Lack of security will affect network level security in infrastructure. Infrastructure security at network level can be done by considering all sources in cryptography .Authorization and authentication can be assured for keeping security.

1-16-- Lack of sufficient security will affect data security. There is chance for intruders to attack database by introducing fraudulent data if there is lack of sufficient data security there by decreasing confidentiality of the customer.

2-16—Lack of data security can cause lack of reliability. If the data obtained from cloud is not correct then the reliability may decreases.

3-11---Network management barriers and lack of portability are related together. Lack of portability means the same software is not able to use in different countries. Portability of the cloud gets diminished due to network management barriers.

4-1—Lack of privacy leads to lack of sufficient security.

4-2—Privacy and reliability are related together.Lack of both will influence cloud services. If the customer is not reliable with cloud services then number of customers will get decreased which will ultimately affect the system.

4-9—Lack of privacy and inefficient backup management are affecting the cloud services. If having a good back up management then even the lost data can be reloaded.

5-6—Comprehensive management tool would help automatic service provisioning, balance workloads and aids with capacity planning and configuration management.

5-8—Lack of data confidentiality is fatal reason of the failure of cloud services. Customers should have very high confidentiality in the services of the cloud. Confidentiality can be increased by providing data security and data integrity.

5-11—Common standard for the cloud is necessary so as to improve portability. Changes in the security requirement may change the topology of network.

6-5—Automatic service provisioning and configuration management are considered. A better standard is necessary for the cloud computing services.

7-14—Weak access control is another problem of cloud computing. Infrastructure security at host level is one of the reasons of weak access control. By providing all securities in all levels of infrastructure this can be remedied.

8-5—Lack of confidentiality of customers may affect cloud services.

9-4—Ineffective back up management may cause serious problems if some data get lost unexpectedly.

9-7-- Access control can manage data, racking of servers, networking and cabling.

10-15—Cost/ time barrier is very essential for close watching of cloud services. Cost of running an industry without using cloud is expensive. Cloud migration is more feasible, realistic and less expensive.

11-12—Network management barriers indirectly cause legal issues.

12-17—some customers depends cloud for storing data. If data integrity is not sustained it may lead to legal issues.

12-18—Lack of data availability make customers feel bad about the services of cloud.

13-7—Infrastructure security at network level should be considered seriously and it may cause weak access control.

13-15—Infrastructure security at network level and application level are very important. Correct measurement should be taken for keeping security in both levels.

14-16—Infrastructure security at host level influence lack of data security.

15-10—Infrastructure security at application level should be considered very serious. Cost/time barrier may depend on it.

16-2—Lack of data security is directly proportional to lack of reliability. Reliability can be increased by providing good security for data in cloud.

17-12—Lack of data integrity may lead to legal issues.

18-12—Lack of data availability can also end in legal issues.

3.9 Step IX: Total interpretive structural model.

Total Interpretive Structural Model is obtained from interpretive matrix and diagraph .The nodes are replaced with boxes having elements. Interpretation is depicted on the side of the links. The Total Interpretive Structural Model is shown in Figure 2.

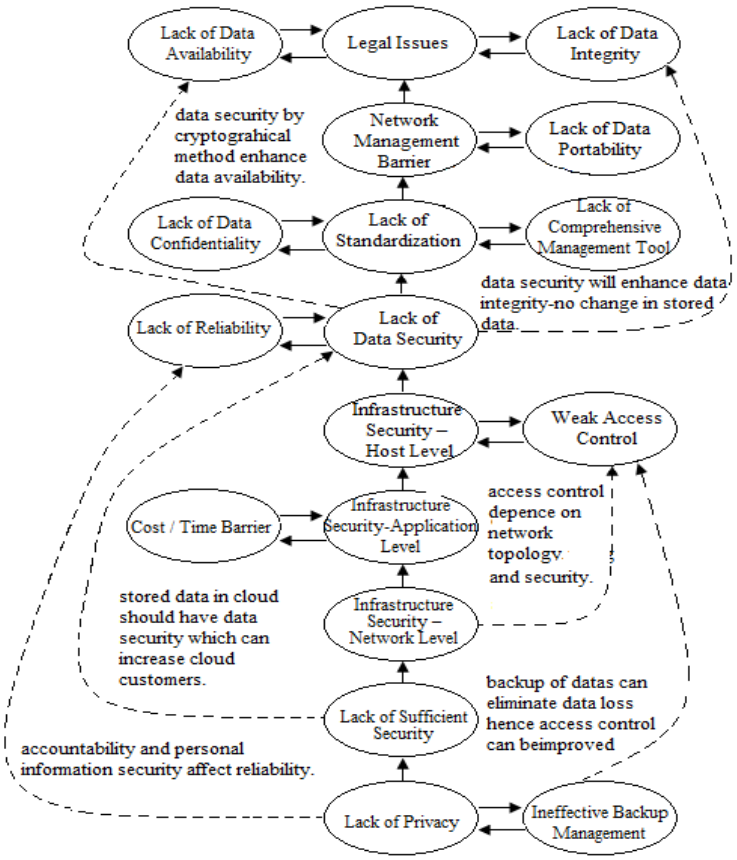

Fig: 2 -Total interpretive structural model

4 Results and discussions

Inhibitors are put in different levels so as to get interrelationship of inhibitors. Level partition is done by considering reachability set, antecedent set and intersection set as described in the section. There are nine Partition levels. The elements coming under each level is discussed below.

The interrelationships of inhibitors are found out from the diagraph. First level elements are legal issues, lack of data integrity, and lack of data availability. The second level elements are network management barriers and lack of portability. Third level elements are lack of standards, lack of confidentiality, and lack of comprehensive management tools. Lack of data security and lack of reliability are under fourth level. Infrastructure security at host level and weak access control are in the fifth level. Infrastructure security at application level and cost/time barrier are in sixth level. Infrastructure security at network

level is coming under seventh level. Lack of sufficient security is coming under eight levels. Lack of privacy and inefficient backup management are in ninth level. Interrelationship among them is shown in the Figure 1. Lack of privacy is very essential and cloud service providers should have to take precautions for it. Inefficient backup management is directly related to weak access control. Lack of privacy is related to lack of reliability, lack of Confidentiality has an indirect relation to data availability. Lack of sufficient security is related to data security. Alidades in cloud should be protected by providing modern concepts of crypto graphical protection. Lack of data security will be directly related to data integrity. Lack of data security affects data availability. Confidentiality level of the customers can be increased by providing data availability and data integrity. Legal issue is related to lack of data integrity and lack of data availability.

5 Conclusion

Inhibitors of cloud computing are studied and their interrelationship is figured out. Interrelationship studied by using ISM has no interpretation for the relation whereas Total Interpretive Structural Modeling has interpretation of the relation. In TISM logic behind the interrelation is clarified through the expert's opinion. Contextual relationship in SSIM remains silent in ISM whereas in TISM the real working is considered. TISM of inhibitors of cloud computing is drawn and the relationship is explained in interaction matrix. Major inhibitors should be considered before going for cloud installation.

REFERENCES

[1]. Tim Mather, SubraKumaraswamy, ShahedLatif, "Cloud Security and Privacy- An Enterprise Perspective on Risks and Compliance" O Reilly

[2]. Wang.C and Wulf W. A., (1997,) "Towards a framework for security measurement", 20th

[3]. National Information Systems Security Conference, Baltimore, MD, pp. 522-533.

[4]. Savola.R and Abie.H, (2010)."Development of measurable security for a distributed

[5]. Messaging system," International Journal on Advances in Security, Vol. 2.

[6]. Jaquith. A, (2007)"Security metrics: replacing fear, uncertainty and doubt,"Addison-Wesley.

[7]. Gadia.S, (2009) "Cloud computing: an auditor's perspective," ISACA Journal, Vol. 6,.

[8]. Gellman.R,(2009) "Privacy in the clouds: risks to privacy and confidentiality from cloud computing," World Privacy Forum (WPF) Report.

[9]. Cloud Security Alliance, (2010) "Top threats to cloud computing", Version 1.0. Downloaded from: www.cloudsecurityalliance.org

[10]. Cloud Security Alliance. www.cloudsecurityalliance.org [July 4, 2010].

[11]. Mandal.A, Deshmukh.S,(1994) Vendor selection using interpretive structural modeling (ism). International Journal of Operations and Production Management, , 14(6): 52–59.

[12]. Sage.A, (1977). Interpretive Structural Modeling: Methodology for Large-scale Systems, 91–164. McGraw-Hill, New York,

[13]. Warfield.J. (2005) Developing interconnection matrices in structural modeling. IEEE Transactionsons on Systems, Man and Cybernetics, 4(1): 81–67.

[14]. Wang.C(2009)"Forrester: A close look at cloud computing security issues," http://www.forrester.com/securityforum

[15]. IDC, "It cloud services user survey, pt.2: Top benefits & challenges," http://blogs.idc.com/ie/?p=210, 2008.

[16]. Zetta, (2008.) "Zetta: Enterprise cloud storage on demand," http://www.zetta.net/,

[17]. Chen.P, Lee.E, Gibson.G, Katz.R, and Patterson.D (1994.) "RAID: High performance,reliable secondary storage," ACM Computing Surveys (CSUR), vol. 26, no. 2,pp. 145–185

[18]. Yahoo!,"Hadoop distribted file system architecture," http://hadoop.apache.org/common/docs/current/hdfs design.html, 2008.

[19]. Dwork.Cet al., "Differential privacy," LECTURE NOTES IN COMPUTER SCIENCE, vol. 4052, p. 1, 2006.

[20]. Dwork.C, "Differential privacy: A survey of results," Lecture Notes in Computer Science, vol. 4978, p. 1, 2008.

[21]. Dean. J and Ghemawat.S,(2004), "MapReduce: simplified data processing on large clusters," in Proceedings of the 6th conference on Symposium onOpearting Systems Design & Implementation-Volume 6 table of contents, pp. 10–10.

[22]. Bardin, (2009.) J"Security Guidance for Critical Areas of Focus in Cloud Computing," www. cloudsecurityalliance.org/ guidance/ csaguide.pdf,

[23]. Hwang, K G. Fox, and Dongarra.J,(2010.) Distributed Systems and Cloud Computing: Clusters, Grids/P2P, and Internet Clouds, Morgan Kaufmann, to appear,

[24]. Nick J,(2010.) " Journey to the Private Cloud: Security and Compliance," tech. presentation, EMC, Tsinghua Univ.,

[25]. Rittinghouse J and Ransome.J, (2010),Cloud Computing: Implementation, Management and Security, CRC Publisher,

[26]. "Gartner Says Cloud Computing Will be as Influential As E-business". Gartner.com. Retrieved 2010-08-22.

[27]. Ravi.V. and Shankar. R. (2005), Analysis of interactions among the barriers of reverse logistics, Technological Forecasting and Social Change, 72(8): 1011-1029.

[28]. Thakkar. J.,Kanda.A. and Deshmukh, S.G.(2008), Interpretive Structural Modeling (ISM) of IT-enablers for Indian manufacturing SMEs', Information management & Computer Security, Vol. 16 No.2, pp. 113-136

[29]. Quan Liu, Lu Gao, Ping Lou, "Resource Management Based on Multi-Agent Technology for Cloud Manufacturing, IEEE 2011

[30]. FarzadSabahi, "Cloud Computing Security Threats and Responses" IEEE, 2011.

[31]. Craig A Lee, " A Perspective on Scientific Cloud Computing", ACM 2010

[32]. P. Sasikala,(2011), " Cloud Computing: present status and the future implications", Inderscience Enterprises Ltd.