FEDERATED CLOUD TRUST MANAGEMENT MODEL FOR EVALUATION AND ESTABLISHMENT OF TRUST IN CLOUD COMPUTING

By

Syeda Hadia Afzaal

Fall2015-MS SYSE 0000117279

Supervisor

Dr. Rabia Latif

Department of Computational Engineering

A thesis submitted in partial fulfillment of the requirements for the

degree of Master of Science in System Engineering (MS SYSE)

In

Research Center for Modeling and Simulation,

National University of Science and Technology (NUST),

Islamabad, Pakistan.

April 2018

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by MS **Syeda Hadia Afzaal,** Registration No. **00000117279**, of **Research Center for Modeling and Simulation** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: _____

Name of Supervisor: Asst. Prof Dr. Rabia Latif, PhD

Date: _____

Signature (HoD): _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

CERTIFICATE

This is to certify that **Syeda Hadia Afzaal**, Student of **MSSE-2** Course Reg. No: **00000117279**, has completed her MS Thesis title **"Federated Cloud Trust Management Model for Evaluation and Establishment of Trust in Cloud Computing"** under my supervision. I have reviewed her final thesis copy and am satisfied with her work.

_____

Thesis Supervisor

(Asst Prof Dr Rabia Latif, PHD)

Dated: _____

ABSTRACT

Cloud computing (CC) is an emerging technology which is used for large scale organizations for data storage and management. It provides advantages like reducing the cost of IT services by shared computing resources and more data storage space, in addition with an on-demand and easy pay per use service mechanism. These emerging developments have a direct influence on many standard parameters like security, trust and privacy etc. On the other side many challenges are also associated with cloud computing that includes, trust establishment, data protection from unauthorized access , data recovery and backup availability when in need and data management capabilities etc. Developing customers trust is considered to be most essential of all. In this regard cloud federation is formed by different Cloud Service providers (CSPs) to share their resources so that they can satisfy their customer's demands and expand their geographic footprints. In cloud environment it is essential to make sure that the customer's data is fully secured and standard privacy laws are applied to form a trusted relationship and estimate the level of trust between the participating CSPs in a federation for the customer's satisfaction. Therefore the focus of this research is to identify the issue for establishment of trusted environment and evaluation of level of trust between CSPs as it is an important requirement for CSPs to take participation in cloud federation for the best utilization of computing resources and customer attraction. The key motivation behind this research is to propose the trust evaluation model that can resolve these issue and motivates the cloud providers to successfully participate in cloud federation. In this regard, a federated cloud trust management model is presented that evaluates the level of trust based on mechanism that considers Service level agreement (SLA) parameters, feedback from customers and feedback from the participating CSPs.

DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

_____

(Syeda Hadia Afzaal)

DEDICATION

This thesis is dedicated to
MY BELOVED PARENTS

AND

HUSBAND

for their love, endless support and encouragement.

ACKNOWLEDGEMENTS

I would thank Allah Almighty for endowing me with His countless blessings. I express my appreciation to my friend Saba Farooq and the faculty for providing their enormous support to help me to do this research. Without their relentless backing, motivation, and prayers, I would not have reached the culmination point.

I extend my deepest gratitude to my supervisor; Assistant Professor Dr. Rabia Lateef, and co supervisor; Assistant Professor Dr. Sana Ajmal, who provided me tremendous support and encouragement for the successful completion of this tedious task.

Finally, I am grateful and thankful to Research Center for Modeling and Simulation (RCMS) and National University of Sciences and Technology (NUST) for providing me the platform and the resources to achieve excellence.

Syeda Hadia Afzaal,

April 2018.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

API	Application programming interface
CSP	Cloud service provider
CC	Cloud Computing
EC2	Amazon Elastic Compute Cloud
FCTMM	Federated Cloud Trust Management Model
FRQ	Federation Request
IaaS	Infrastructure as a Service
IT	Information Technology
LOT	Level of Trust
NASA	National Aeronautics and Space Administration
PaaS	Platform as a Service
PC	Personal Computer
QoS	Quality of Services
ROT	Range of Trust
S3	Amazon storage service
SaaS	Software as a Service
SLA	Service Level Agreement
SQL	Structured Query Language
TEM	Trust Evaluation Model
TMM	Trust Management Model
TRQ	Trust Request
TRS	Trust Response
TST	Trust Statement
WSN	Wireless Sensor Network

NOTATIONS

N_l	Total no of levels defined
N_p	Total no of parameters
L_i	Level given
SP_i	Security Parameter
m	Margin of error
τ	Threshold
S_{SLA}	Total score of SLA module
F_T	Total no of features
W_i	Weight given by model
$peer_i$	Score given by peer participating
T_f	Total score of a defined Feature
S_{CLOUD}	Total score of cloud module
T_{peer}	Total no of peers participating
T_{csp}^{C}	Trust score given by customer about CSP
p_r	Positive response
n_r	Negative response
U_f	Uncertain response
N_s	Total no of scales defined

Chapter 1

INTRODUCTION

1.1 Introduction

This Chapter gives the overview of the importance of Cloud Computing and identifies the main issues related to it. It concisely highlights the relevance of customers trust in cloud environment. The chapter explains the main motivation for carrying out the research work in cloud Computing. It highlights the key objectives. Finally the chapter ends by discussing the organization and structure of thesis.

Now a days Cloud Computing is an emerging technology for large scale organizations. It introduces many advantages like reducing the cost of IT services by shared computing resources and more storage space, in addition with an on-demand service mechanism based on an easy pay-per-use system. These new developments have a direct influence not only on the costing of IT but it also have a huge impact on many standard parameters like security, trust and privacy etc.

Many challenges are associated with cloud computing that includes, trust establishment, data protection from unauthorized access, data recovery and backup availability when in need and data management capabilities etc. Trust is a very important term which is used in a person's social life. The level of trust in our everyday life is measured by factors like mutual co-operation, good relationships and strong coordination. With time this social trust is greatly affected by new experiences and changed according to the circumstances we face. With the emergence of internet and networking technologies, trust has been a substantial factor of design and implementation of secure information systems and distributed computing. When the concept of trust emerged in the digital world, the legal frameworks were introduced as a standard to create and initialize trusted relationships between business organizations and financial transactions. Trust is referred as an abstract and subjective term. In cloud infrastructure, it is the process of recognition of a cloud provider/user identity and the confidence on its behavior. Trust can be achieved through trust mechanisms by applying trust models. A trust model is basically a protocol or management method that includes factors like trust establishment, trust renewal and trust withdrawal. Trust management in cloud computing infrastructure cannot be performed

with the conventional trust models because cloud infrastructure includes certain characteristics for example their size, location, lack of perimeter, number of users and lack of confidence etc. [1]

Using CC technology one of the biggest challenges is the user's level of trust in cloud service providers. Security should be created properly otherwise the concept of cloud infrastructure would flop badly as the concept of cloud computing includes managing sensitive data of its users over a network which provide services. This statement is supported by a survey [2] conducted by the Fujitsu Corporation, 88% of customers, worldwide, are concerned about the privacy of their data and almost the same percentage of customers are concerned about the blind storage location of their data as in cloud computing as the actual data storage location is not known to its customers. CSP's which provide any services (Iaas, Paas, Saas) need effective methods to enhance trusted cloud environment which will help to draw more customers towards this technology and ensure data security to those customers.

Due to this demanding technology and its rapid growth more users and organizations are shifting towards cloud. Cloud federation brought an old idea into new concept. It allows CSP to share their resources for load balancing and scalability. In cloud federation, migrating data from home to foreign CSPs domain brings security and privacy concerns for cloud consumers. In order to make sure that the customer's data at foreign CSPs platform is safe, there is need to evaluate and establish trust between both participating CSP's. In this regard, an excessive work has been done for evaluation and establishment of trust in CC, however trust issues still emerge in cloud federation with more advance risks. These trust models are used to evaluate the level of trust of CSPs based on certain factors and establish trust between two CSPs participating in federation. The basic concept of cloud federation is depicted in figure 1.1

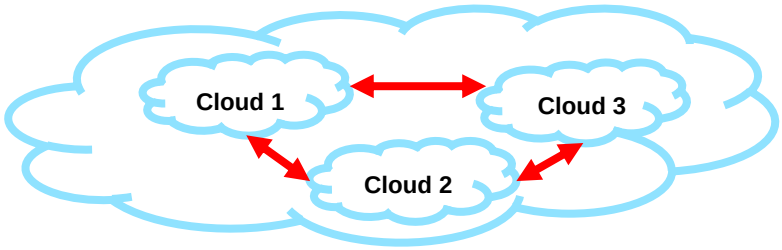

Fig 1.1: Cloud Federation

1.2 Research Significance

This research will focus on the privacy, security and trust issues in federated cloud environments and will provide a topic that should be considered as a significant issue by the future researchers. Along with this the research will provide the guidance to CSP who want to form federation by evaluating trust of each other which helps to ensure the customer's data is secured.

1.3 Relevance to National Needs

Our organizations have fully transformed towards Information technology and CC technology to access on demand resources. They need to trust on CSP and consider the following aspects

- Who the provider is?
- Is it secured?
- To which level it is secured?

To answer those questions they need a proper trust evaluation model. So this research plays an important role by providing a mechanism for establishment and evaluation of trust based on multiple factors in cloud federation.

1.4 Motivation and Problem Statement

CC has proved to be a revolution in the world that is accompanied by the upcoming concept of cloud federation. Shortly the mechanism of cloud federation has proved to be an advantage for various CSP, whether small or large scale, to conveniently share their provided services to gain profits and expanding their business. This can be all done without setting their own computing resources. Cloud federation mechanism allows a CSP to utilize the resources of other CSP when the requirements exceeds a level and let a CSP utilize resources when other cloud providers wants to share their burden. When a CSP has less resources it can use resources on-payment in the computing infrastructure of another available CSP which is ready to share its unused capacity of resources. Despite of numerous advantages, the cloud federation mechanism is also has major hindrances that includes the following

- Optimum resources allocation for better management,

- Discovery of available resources for load balancing,
- Dynamic resource provisioning,
- Establishment of trust for customer satisfaction, and
- Interoperable security

The main challenge in cloud federation due to which CSPs or user hesitate to participate in Figure 1.2 shows low level of trust between the cloud federation and the cloud providers.

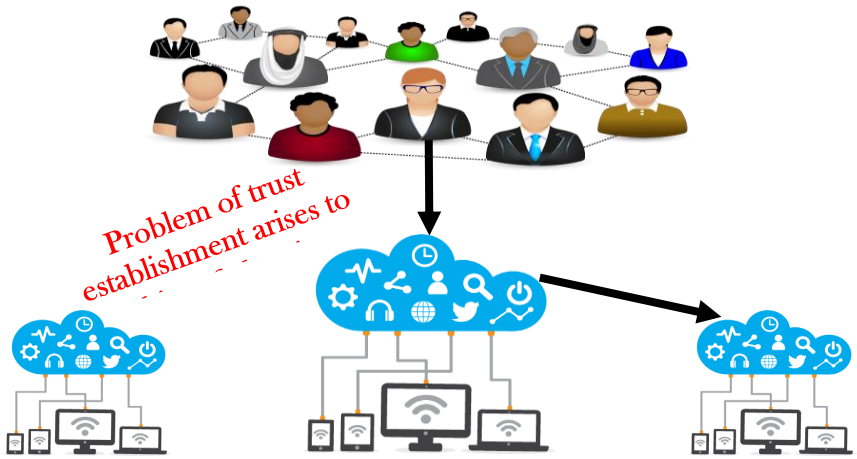

Fig 1.2: Trust Establishment in Cloud Federation.

In cloud federation, when customer's or CSP's requests for service simultaneously, these requests are redirected because of exceeding demand from one CSP to another CSP. Due to this the sensitive data items or even the complete virtual machine is migrated from one CSP to other cloud platform. Now, to make sure that the customer data is fully secured and standard privacy laws are applied, it is essential to form a trusted relationship and estimate the level of trust between the participating CSPs who want to make a reliable federation for the customer's satisfaction [31]. Therefore trust is expected between the clouds participated in federation. So we identified the issue of establishment of trusted environment and evaluation of level of trust between CSPs as it is an important requirement and become a necessity to take participation in cloud federation for the best utilization of computing resources [32]. In this respect, the main motivation for this research is to propose trust evaluation model that can resolve this issue and helps the cloud providers to successfully participate in cloud federation and utilize the best of their resource.

1.5 Contributions and Outcomes

This thesis made several contributions which are enlisted below with their brief description and shown in figure 1.3.

- **Contribution 1**: Comprehensive analyses of Trust Management Models already proposed for evaluation of trust between CSPs in federated environment.
- **Contribution 2:** Proposed a Federated Cloud Trust Management Model (FCTMM) for CSP to ensure the security of critical and sensitive data of their customers and participate in reliable federated environment.
- **Contribution 3:** Implementation and evaluation of the proposed FCTMM and comparison with the existing techniques.

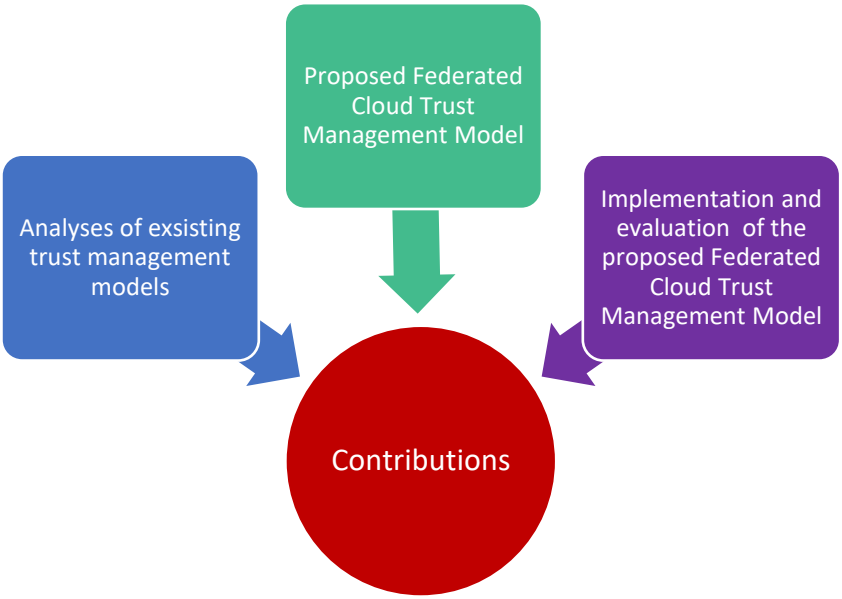

Fig 1.3: Thesis Contributions and outcomes

1.6 Thesis Outline

The thesis is structured as follows:

- **Chapter 2** discusses the basic concepts and history of cloud technology. CC service delivery models and deployment models along with the security challenges. Along with this different existing techniques and methods used to evaluate trust in cloud environment. The comparative analysis of these techniques is carried out and the shortcomings present in them have been reported.

- **Chapter 3** discusses the proposed FCTMM along with its key components and implementation technique. The design along with architecture of purposed trust model is presented. Details of individual modules is also the part of this chapter.
- **Chapter 4** discusses the implementation mechanism of the proposed FCTMM and the obtained results are also discussed.
- **Chapter 5** will summarize the whole research work and will notify the conclusions drawn during the thesis. This chapter will end the thesis while highlighting the academic and industrial importance and more research directions in accordance to this thesis.

1.7 Conclusion

The objective and motivation to conduct the research on cloud federation has been described in this chapter. The research methodology developed during the research is also mentioned. Its importance for academics, industry and military has also been highlighted. At the end it describes the overall structural organization of the thesis.

Chapter 2

LITERATURE REVIEW

2.1 Introduction

This chapter briefs about the basic concepts and history of CC. This chapter also elaborates about the characteristics of CC along with the literature work which has been carried out. CC service models and deployment models are discussed. Significant security challenges are also highlighted in this section. Concept of trust, its history and existing trust models in cloud computing is the part of this chapter.

The concept of CC is actually introduced by McCarthy in 1960's. The term "Cloud computing" is a mix of two important words "Cloud" and "computing", where cloud is used for Internet [1]. So, the term CC is "computing based on internet" in which different types of services mainly applications, data servers, software and network equipment are readily available to the provide services to customers over the internet.

It facilitates with the services over the internet rather than managing the computing resources on local servers which has a limited scope. It provides the advantage of online subscribed available services instead of installing and managing the required applications on local servers. With this emerging internet-based technology, the cost of IT resources, application hosting, and data storage and information delivery is reduced significantly. The cloud computing architecture is shown in figure 2.1.

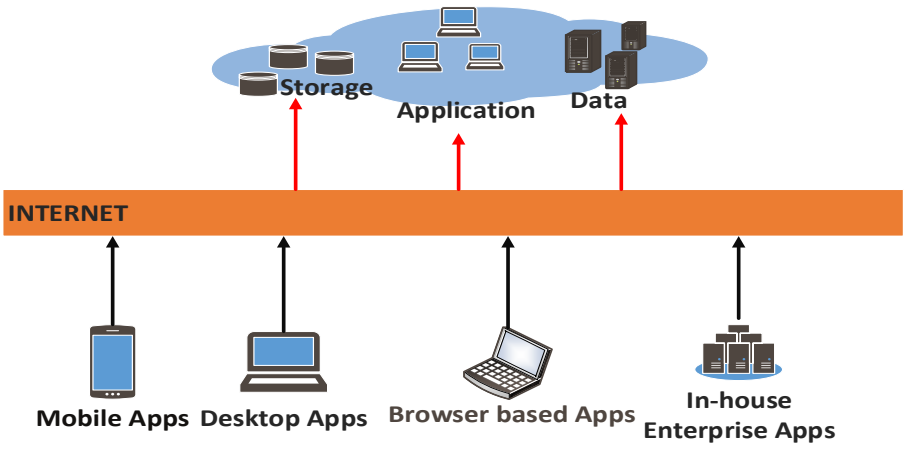

Fig 2.1: Cloud computing architecture

2.2 Characteristics of Cloud Computing

There are many characteristics of CC that makes this technology different from the traditional computing approaches, significant ones are listed below and also as depicted in figure 2.2

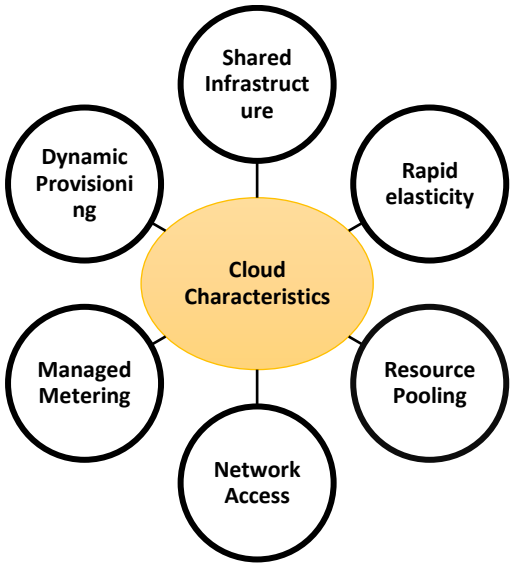

Fig 2.2: Characteristics of cloud Computing

2.2.1 Shared Infrastructure

Through the use of a virtualized infrastructure, the sharing of physical resource services, data storage, and networking competencies are made easy. The cloud mechanism comprises of the available infrastructure across a large number of registered users [3].

2.2.2 Provisioning dynamically

It enables on-demand services that are based upon the customers' requirements. This task is done through a software automation mechanism. This dynamic provisioning is done while considering reliability and security aspects [3].

2.2.3 Network Access

As CC is accessed from a broad range of devices using internet. These devices may include PCs (Personal Computers), laptops, and mobile that uses standards-based APIs (Application programming interface). Hence providing cloud services to large number of

users. These cloud services includes large range of applications from business purpose applications to the versatile applications on the latest available devices [3].

2.2.4 Managed Metering

Metering is used for the management and optimization the on-demand services and to provide reports and bills data of the users. In this regard, consumers are billed only for services based on the actual use of service during the billing time. In CC, sharing and scalable deployment of services is made available and is also allowed as per need, from any location, and for which the customer are only billed according to their actual usage [3].

a) Resource Pooling:

Different computing resources (physical and logical) are combined in multi-tenant cloud environment to aid the multiple consumers at a time. All these resources can be allocated and de-allocated in according to the customer's requests for services. In cloud environment the costumer is unaware of the actual location of various types of allocated resources which are used for storage, processing, virtual machines or network bandwidth [3].

b) Rapid elasticity*:*

In cloud environment the computing resources can quickly scale out and scale in according to the customers demand. These elastic capabilities are unlimited to the Cloud customers and can be availed at any time when needed [3].

2.3 Cloud Computing Service Models

In CC environment all of the services are provided at certain level of abstraction to consumers. Cloud providers offer their service to the consumers using three of the main services models which are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) as depicted in figure 2.3

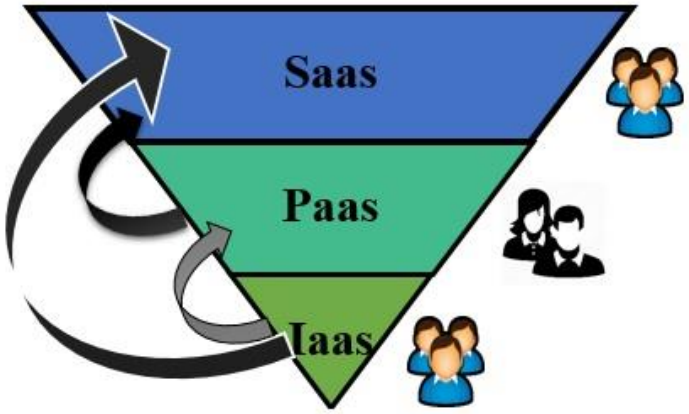

Fig 2.3: Cloud Computing Service Models [4]

2.3.1 Software as a Service (SaaS):

In this Service model**,** on demand cloud services are made available to the customer at application level. A single service application runs on the cloud & numerous customers are serviced simultaneously. From the consumers perspective there is no need to install and run the required software at their local systems. Whereas form the providers perspective, the costs are lowered for hosting and maintain the software. Examples of SaaS offered by CSP's are Google, Salesforce, Microsoft, Zoho etc. [4].

2.3.2 Platform as a Service (PaaS):

It is an extension of SaaS model because along with the application layer it also includes the operating system layer. In this model a layer encapsulated software is offered as a service, which can be used to build other higher levels of services. The customer have a choice to design his own required applications, which run on the infrastructure built by the provider. To meet the basic requirements such as manageability and scalability of the applications, PaaS providers offer a blend of OS and application servers which is predefined. Some of the popular PaaS examples are Google's App Engine, Force.com, etc. [4].

2.3.3 Infrastructure as a Service (Iaas):

This model provides the customer with a complete infrastructure to its consumers. It provides basic capabilities such as storage and computing as a standardized services over the network. Servers for computation, storage systems for data, networking equipment for data processing, data centers are shared and made readily available to handle workloads efficiently. It reduces the cost of purchasing dedicated servers and the maintenance of equipment. The customer is free to install his own software on the infrastructure. Examples of Iaas are Amazon, Go Grid, Tera, etc. [4].

2.4 Cloud Computing Deployment Model

The cloud deployment models shows the details regarding the deployment and management of actual cloud servers. Several cloud deployment models with examples are depicted in figure 2.4

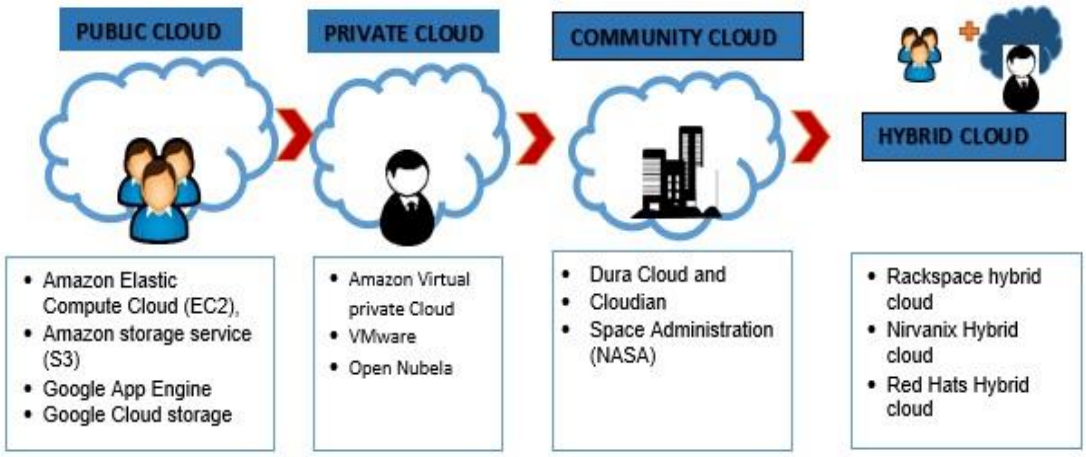

Fig 2.4: Cloud computing Deployment Model with Examples

2.4.1 Public Cloud Deployment Model:

In cloud infrastructure Public clouds are those which are owned and operated by a mediator, they provide highly cost effective approach to customers, cloud infrastructure costs are spread among a number of customers, providing each customer a cost effective, “Pay-as-you-go” mechanism. All customers share the same set-up with pool of resources. This type of infrastructure is usually recommended by the cloud provider. The prominent

advantages of a Public cloud is that due to its vast foot prints it provides an ability to scale seamlessly, on demand. Due to this many security and trust issues arises for cloud consumers which prove to be a disadvantage. The level of trust on public clouds reduces because the model provide no details about the storage and management of critical data [4].

2.4.2 Private Cloud Deployment Model:

This deployment model is built and deployed solely for a single enterprise at a time. This model aim to resolve the issues faced in public clouds such as data security and trust issues and propose a complete data control within the enterprise. There are generally two types of private cloud infrastructure which are listed below:

a) On premise Private Cloud Model*:*

These deployment models are also called internal clouds that are deployed within the organizations private data center. Due to this the deployment model offers a more reliable and trusted process, but it has limitations with respect to the size and scalability concerns. The costs (capital and operational) for the service resources become high. This infrastructure is best considered for applications that need a full control and configurability of the customer's data whose data needs high security level [4].

b) Externally hosted Private Cloud Model*:*

This is a type of private cloud that is deployed outside the organization with the help of a cloud provider with the help of an exclusive cloud environment to the customer with complete assurance of privacy and security of data. This used for enterprises whose environments do not prefer a public cloud infrastructure due to shared service resources [4].

2.4.3 Community Cloud Deployment Model:

In this type of infrastructure different organizations having mutual policies, procedures and security parameters are grouped together to share the resources. It proves to be more cost effective as compared to deploy a private cloud because the organizations have similar aspects like business procedures, data storage, data control and information sharing requirements. This deployment model can be handled by organizations themselves

also known as on-site handling or some third party provider known as off-site handling. It offers the mutual features of private and public clouds which includes applications, secure data management and computing resources which are consumed by several organizations participating in that infrastructure [4].

2.4.4 Hybrid Cloud Deployment Model:

Hybrid clouds combines both public and private infrastructures as well as community cloud to form a cloud team. The communication among clouds is done using different APIs and secure communication channels. The advantage of this model is that the organizations gets security and privacy parameters like the private cloud infrastructure along with reduced cost and high availability. Thus, it provides more flexibility and scalability [4].

2.5 Security Challenges in Cloud Environment

As discussed earlier CC has many advantages but have many security and privacy concerns as well that hinder the cloud infrastructure implementation by various IT organizations. The main security concerns include aspects as Data confidentiality, data privacy, identity management and trust establishment. Issues related to cloud computing are shown in figure 2.5 and are discussed below.

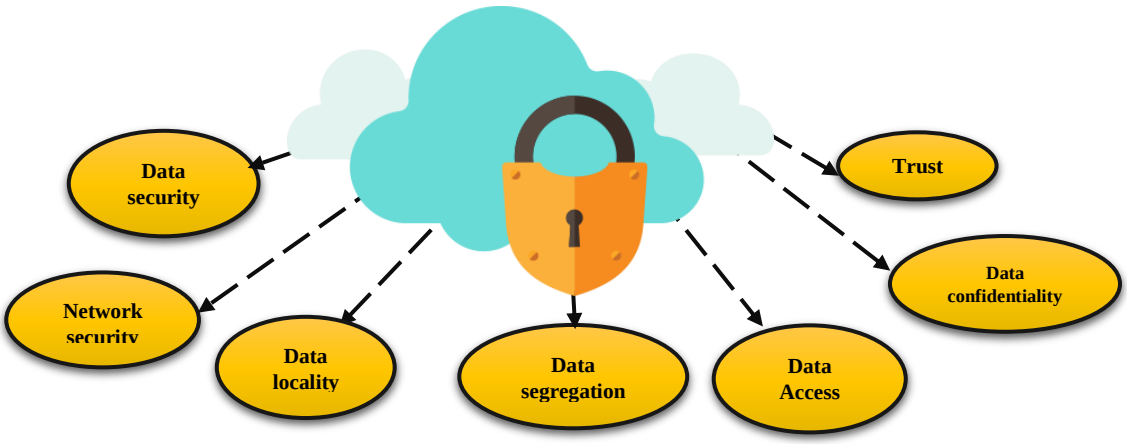

Fig 2.5: Cloud Computing Security Challenges

a) Data security:

In an enterprise, the sensitive data stays within the local boundaries of organization due to security reasons. When converted to cloud platform, the cloud providers have to pay attention to the management of additional security checks to prevent data from any sort of attacks and security breach. Different techniques as cryptography, encryption and access control mechanisms are adopted to secure the data [5].

b) Network security:

As communication over internet involves flow of consumer's data through the network, therefore while considering security issues in CC, network security is also an important issue to be considered. This includes protecting the customer's data over network by using of advanced techniques of network security like encryption techniques and many more can be implemented to protect customer's data over the network provided [5]

c) Data locality:

Numerous cloud consumers and business organizations set up their applications and data on cloud to get benefit from various flexible and on demand services by cloud providers. As in cloud environment cloud customers are totally uninformed of actual location of their data, this transparency arises many privacy and security concerns. As data protection laws and policy varies countries to country, therefore data locality is an important concern for many organizations. When organizations data crosses boundaries for storage or access purpose, it may arise compliance and privacy issues for the enterprises [5].

d) Data segregation:

The CC environment includes multi-tenancy to its customers which causes data from different customers to reside on same physical location. As the data location is shared security concerns arise as one consumer can damage the data of another consumer by introducing malicious codes or any other kind of virus to the system. So to provide complete data segregation in cloud environment, some implementations are needed at application level like SQL (structured query language) injection flaws, data validation mechanisms [5].

e) Data Access:

Due to security policies provided by an organization to its consumers data access issues occur. Every organization has established a set of security policies for its customers. Cloud providers should also be support these security policies to avoid any security breach to the critical data. Proper authentication and authorization mechanisms are implemented to ensure the privacy and security to customer's data [5].

f) Data confidentiality:

In the cloud domain this term relates to the competence of sharing data among a pool of customers within the cloud environment while keeping in mind the rights given by the owner of data to each participating user of the community. Any user who is outside the community is considered to have no rights. To avail the IaaS services in cloud environment, the cloud consumer subscribe for the cloud services where their data is transferred out of the organization's boundary due to which data confidentiality issues arise in an organization [5].

g) Level of Trust:

Level of Trust in CC depends on the type deployment model used, as in cloud mechanism the critical data and applications are totally transparent and completely not in hands of the owner's control [22]. Cloud provider do not show the data storage location and maintenance procedural details to its customers because of the vast geographic footprints, this cause many trust related issues to rise. To select a CSP with completely trusted and suitable parameters is the most important challenging issue in such environment. Moreover the level of trust may fluctuate with time due to experiences gained, new aspects of knowledge and outside opinion involved. Hence, to build trust between customer and targeted CSP, a formal agreement stating all the standard parameters is put forward and signed which is technically known as Service Level Agreement (SLA) [25]. SLA format varies from one organization to another so it cannot be considered as a trust parameter.

2.6 Trust Models - Overview and History

A trust model is a technique which is used to evaluate, formulate and set up the trust relationships among different entities. The very first trust model was presented by Marsh in 1994 which includes the integration of various features of trust from the disciplines of sociology, economics and commerce [6]. This concept brought the understanding of how to measure the trust in digital form. After presenting this concept many other trust models emerged for different areas of computing which mainly includes peer-to-peer networking, ubiquitous computing, ad hoc networks, multi-agent systems and CC. This concept by Marsh was extended by another researcher Rahman in 2000, where the focus was given to virtual online communities to evaluate the trust using large amount of knowledge gathered by the participants [7].

In 1999 a survey was conducted by Hoffman and Novak more than 95% of the web users were reluctant to shop online because of lack of trust on these business organizations. The reason behind these results was that the users feel less secure with respect to their personal information used during the transactions they make [8]. For this purpose a trust evaluation model was introduced based on control and subjective trust to make the secure and reliable transactions between users and business organizations by building the online trust. In 2000, Machala has proposed few advance trust evaluation metrics that can be used for measurement of online trust in the field of e-commerce [9].

Now a day's important domain where trust models play vital role is in distributed computing which includes mobile networking, wireless communication, ad hoc networks setup, peer-to-peer networking and Grid computing [10][11]. All these areas are highly vulnerable to security breach due to lack of trust between different nodes of a sharing the information for various purposes. In this regard Tajeddine et al. have proposed a trust reputation model for distributed systems for the participating entities [12]. A reputation value is formulized using the past interactions with that entity and a final decision is made whether to continue the communication or abort it based on it. Cuboid a reputation based Trust model is also presented in 2007 for peer-to-peer networking which formulates the trust for a specific peer based on the feedback given by other participant peers in network [13]. After the emergence of CC mechanism trust is considered to be the most challenging

issue faced by different cloud consumers as well as cloud providers. In this regard, different cloud based trust models have been proposed that establish the trust between Cloud consumers and CSPs.

2.7 Level of Trust in Cloud computing

In such environment the establishment of trust between the cloud providers and consumers and also between two cloud providers is a great concern. The situation become more critical when consumer's data is distributed across various geographical locations and becomes invisible to the owner. We can take an example of a Telecom enterprise that needs to outsource the application for storage of customer's records at cloud platform. The main purpose of this application is to reduce the costs required for maintenance, storage, IT peripherals etc. This application uses the personal records of customers that need to be maintain and stored on most reliable and secure cloud provider among all. The Telecom enterprise will require assurance about the privacy and security records stored as well as high availability and best Quality of Services (QoS). With the increase use of internet and growing awareness in this field the CC market is expanding more and more to ease the customers. Due to this a large number of competitive service providers have been emerged. In this case, such Telecom enterprise has to select the best suited and appropriate CSP among them by comparing the features offered by the CSP's. To facilitate in such circumstances various trust establishment mechanisms are proposed that includes the SLAs, Reputation or trust policies [7] [8] [9].

2.8 Existing Schemes To Evaluate Trust in Cloud Computing

The detailed analysis identified the publications that contained some trust establishment models in CC is shown in table 2.1. It consists of the results of reviews and analysis of the existing solutions to evaluate trust in CC environment. It can be concluded from the studied literature that the existing models have some strengths as well as weaknesses. So there is a need to propose a model that could overcome the flaws of the existing schemes in order to evaluate trust between CSPs in federated environment.

Table 2.1: Reviews and analysis of the existing solutions

Year	Authors	Paper Name	Review	Analysis
2017	U.S. Premarathne, et al. [14]	**Cloud-Based Utility Service Framework for Trust Negotiations Using Federated Identity Management**	Proposed a model for establishment of trust between the CSP and the identity providers.	Lacking security and privacy requirements for a service operation.
2016	B. Suzic et al. [15]	**Towards Secure Collaboration in Federated Cloud Environments**	Presented an ongoing work that establishes the enforcement of data security in cross-organizational domain.	Proposed framework is closed to all the external Parties thus the proposed model offers limited data sharing.
2015	S. Jafari and et al. [16]	**A Multi-factor Trust Management System Based On Confidence In M-commerce Environment**	Proposed system which uses factor of confidence in calculating trust values.	Different types of threatening attacks of the proposed trust management system are not included.
2014	A. Kanwal et al. [17]	**Evaluation and Establishment of Trust in Cloud Federation**	Proposed a trust evaluation framework by using different underlying protocol for trust calculation.	Only includes the trust of individual CSP and parameters taken are limited.
2014	S. Singh et al. [28]	**Trust Evaluation in Cloud based on Friends and Third Party's Recommendations**	Proposed CSP rust evaluation framework from three different angles which includes self-trust, friend trust and third party trust.	Only calculates trust based on recommendations.
2013	F. Rajibabaei et al. [18]	**Proposing A Centralized Trust Management System To Detect Compromised Node In WSN (wireless sensor network).**	Proposed a trust management model in WSN in which uses sink nodes mechanism to determine trust values of nodes by nodes control information.	Only consider routing attacks.
2012	S. Chakraborty et al. [19]	**An SLA-based Framework for Estimating Trustworthiness of a Cloud.**	Proposed a framework to calculate the consumer level of trust on CSP.	SLA features considered are limited.
2011	D. Wallom et al. [20]	**Trusted Cloud Infrastructure for Security-critical**	The paper illustrates a use case scenario of Trusted Computing Technologies	Limited to business-critical applications only.

		Computation and Data Management.	into an accessible cloud infrastructure.	
2011	S. K. Garg et al. [29]	**SMICloud: A Framework for Comparing and Ranking Cloud Services**	Proposed a systematic framework to measure QoS attributes Provided by CSMIC and rank the Cloud services based on the provided attributes.	Do not manage the variation in QoS attributes.
2011	S.M. Habib et al. [21]	**Towards a Trust Management System for Cloud Computing.**	Proposed an architecture of a Trust Management model to differentiate between the qualities of providers to help cloud customers.	Management and update mechanisms are not considered.
2010	S.M. Habib et al. [22]	**Cloud Computing Landscape and Research Challenges regarding Trust and Reputation.**	The paper portrayed the landscape of Cloud Computing from the customer's viewpoint and pinpoints the research challenges regarding cloud trust level.	Theory based research, only considers from customers point of view.
2010	M Alhamad et al. [23]	**SLA-Based Trust Model for Cloud Computing.**	Proposed a SLA based trust model to weigh cloud services to facilitate cloud users in selection of the most reliable resource.	Only from users point of view and limited parameters are considered.

In this research paper [14] the authors proposed a cloud trust architecture for considerations on federated identity management mechanism. Different Fuzzy models are used for the development of framework. An evidence based cooperativeness evaluation strategy was also presented which includes two metrics, trust metrics and policy dependency cost metric to approximation of reliability level of identity providers. The results show that this model is reliable enough for trust negotiations.

B. Suzic et al. [15] presented a security model for cloud federation that enables cloud to increased service efficiency, data reliability, and complete control of their infrastructures. Additional requirements such as data security and privacy are also included. In the presented model, the cloud federation is formed from zones with similar requirements on data security. Transparent gateways are used to govern the access between

zones, while zone-members are responsible for the policy control through which data is accessed through zones.

In this paper [16] S. Jafari et al. presented a cloud trust architecture for mobile commerce environment. The system detects fraud and searches for more reliable provider. In the paper risk factors of m-commerce systems are mentioned and counter strategies are considered to mitigate the trust. The model calculates the degree of confidence based on level of trust Results indicates that the proposed trust architecture can reduce estimation error significantly and prove its efficiency.

In this paper [17] A. Kanwal have proposed a trust calculation model that eases the CSPs to weigh the level of trust and enable them to share resources in a trusted and reliable federated Cloud environment. The calculation is based on two main mechanism for trust estimation that are feedback from users and SLAs. SLA parsing extract the required parameters. An combined level of trust value is evaluated using these mechanism. These trust values are then swapped between home and foreign CSPs.

F. Rajibabaei et al. [18] Proposed a trust evaluation method in which sink mechanism is used. It can sense a nodes values as it received control information of each node. Results show high level of accuracy as sink node has a view of the network architecture thus a malicious node is not able to create different values. As sink node has enough memory capacity, it can store long history of nodes and as use it to res effectively detect attack.

S. Chakraborty et al. [19], presented a work to estimate the level of confidence a user can have on the service provided by CSP. The presented method collects parameters from SLA and comparable documents and then evaluate reliability of parameters. Criteria for selecting chosen parameters is that they could qualify for overall quality of the CSP. It is flexible as the trust level can be adjusted by adding more to parameters and incorporate expert opinions. The framework can calculates trust as per individual consumer's policies.

In this paper [20] the authors have presented a trust-capable cloud infrastructure in UK which is based upon available public cloud infrastructure. The method presented in the paper is combined in such a way that the lowest level of virtualization software is

considered. It will work for any of the open source cloud solutions. The application proves that the platform is a feasible solution for the security requirements of the transmission and distribution network business sector in UK.

S.M. Habib et al. [21] Proposed a Trust Management model to efficiently compare between a good and a poor quality providers. The method is fabricated to provide a tailored trust level of the cloud provider which depends upon the features selected on basis of the customers demand. The method also provides trust values of the CSP's which depends upon two factors, first is the trustworthy behavior of the underlying systems and other is questionnaire. The aggregate trust value is presented in numbers and a graphical interface.

S.M. Habib et al. [22] Depicted the landscape of CC and the services fulfilled by the cloud providers now a days. The significant benefits are discussed and possible threats and risks from the customers' perspective in CC environment are identified. The paper discusses a lot of research challenges in CC about SLA specifications, authorizations, open standards, security measures, and service selection.

M Alhamad et al. [23] presented another trust model that includes standardized criteria for the service level agreements and user understandings to determine the level of trust upon cloud providers. The presented model can be applied upon different nature of cloud services offered so that the specific users can acquire a more desirable trust level for the same services used.

In this paper [28] S. Singh et al. propose a trusted technique to calculate trust values of cloud service providers. The framework calculates final trust value which is based on consumer's self-trust on CSP, friends' trust on CSP and third party's trust on CSP. The results indicate that the framework can be used to evaluate trust of CSP.

In this paper [29] S. K. Garg et al. proposed a framework which is based on mutual features provided by the cloud services providers. Each of QoS attributes given is defined in the framework and provides a systematic methodology for calculating a relative index for comparing each cloud services provided by the CSP. This index is then used to rank each CSP accordingly.

2.9 Conclusion

In this chapter we have highlighted various concepts and history of CC. Cloud computing delivery and deployment models are also discussed. At the end of the chapter review and analysis of various existing techniques is done along with their relative comparison with respect to the parameters used for trust evaluation. The next chapter will focus on the proposed FCTMM implementation techniques.

Chapter 3

PROPOSED FCTMM FRAMEWORK

3.1 Introduction

This chapter includes most important discussion about our proposed trust evaluation model for establishment of trusted cloud federation. The proposed trust model will evaluate and establish trust between user and CSPs, and also between two CSP's in order to provide the trusted and reliable cloud federation. The design along with architecture of purposed trust model is discussed. Details of individual modules are also discussed.

3.2 Proposed Framework of FCTMM for Evaluation and Establishment of Trust in Cloud Computing.

We propose a FCTMM for evaluation and establishment of trust in a cloud federated environment as shown in figure 3.1. The proposed model mainly includes three mechanisms, SLA parameters, feedback from users and feedback from neighboring clouds. Today the use of cloud mechanism is increasing day by day .Every organization is shifting their data to cloud environment. So the main task of the proposed mechanism is to evaluate the level of trust and establish trusted relationship between CSPs to facilitate them in order to provide a reliable and secure mechanism in federated cloud environment and to their customers as well. In the presented model, trust is taken as an arithmetic value which lies between 0 and 1 [33].This value is used to define the range of trust first(between 1 and 0) and then the level of trust (high, medium and low) of a targeted CSP accordingly. The final score of trust accumulated is evaluated using scores from individual mechanisms that terms the overall level of trustworthiness of the targeted CSP accordingly.

In the next section we will discuss the proposed architecture of our FCTMM and its complete workflow, sequence of actions to estimate the trust scores gained individually as well as the final trust score The proposed FCTMM considered as a trusted third party that help to evaluate the trust scores of the participating CSPs on receiving the requests from them in federated environment

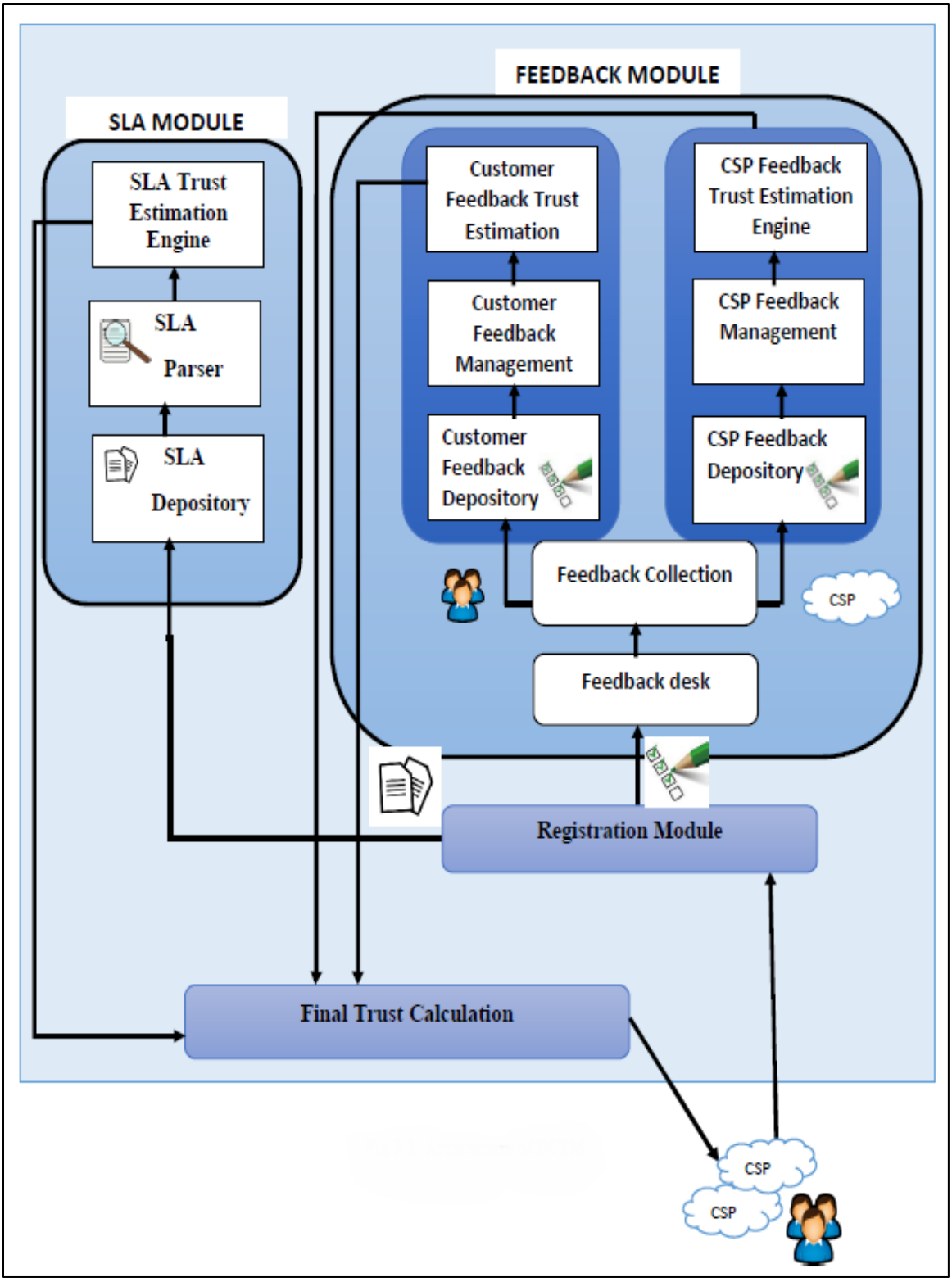

Fig 3.1: Architecture of the proposed FCTMM

3.3 Work Flow of FCTMM

The complete workflow of the proposed FCTMM is shown in figure 3.2.

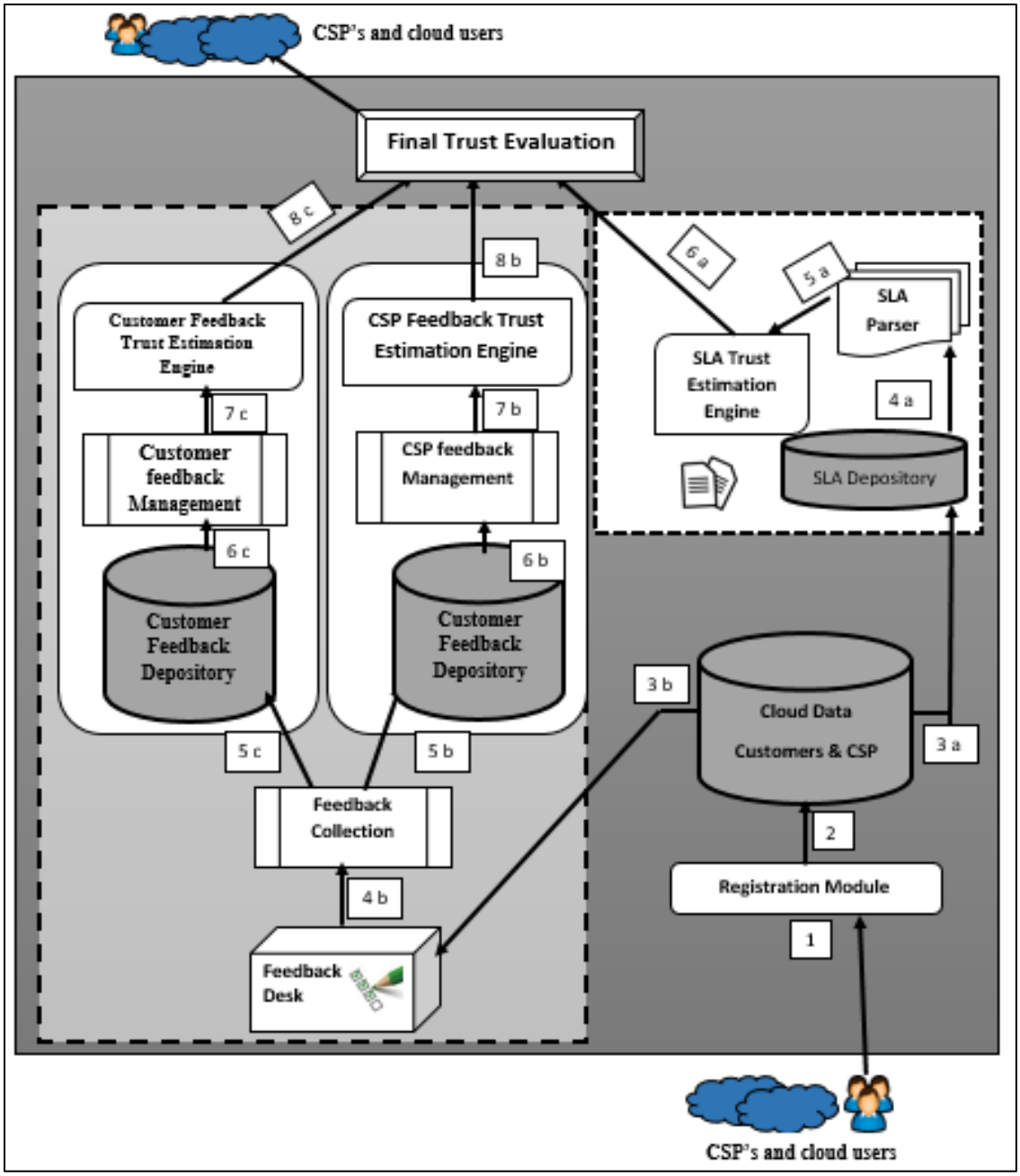

Fig 3.2: Work flow for the proposed FCTMM

The first step starts when the CSPs and their customers who want to participate in secure and reliable cloud federation, register for the trust evaluation model. The registration module asked them to submit the required authorizations that include basic data of

registering customers, SLAs of CSPs and CSP's basic information about their certain parameters.

The SLAs of registered CSPs that are collected by the SLA module are first submitted to the SLA depository where all the data is stored. The SLA's are then send to SLA parser where the SLA are examined according to the set parameters that are defined in the security and privacy domains that are discussed later. The extracted parameters are then evaluated and the trust score is calculated in the SLA trust evaluation engine.

The information is then passed to the feedback module. The information is first send to feedback desk where it differentiates between the feedback request form user and CSP. Then the feedback collection module ask for feedback from CSP and user individually. If the feedback is from user then send it to user feedback module and if it's from CSP it send the information to feedback from CSP feedback module.

If the feedback is from the user the user the information goes to the user feedback depository. The user Feedback module collects the feedback in form of a questionnaire. The questionnaire contains different types of questions regarding security and privacy features from the user aspect. Then the final trust score is evaluated in the User Feedback Trust Estimation Engine. If the feedback is from CSP then the information goes to the CSP feedback module. The information regarding CSP is submitted to CSP feedback depository. Then the CSP feedback management presents a questionnaire for the participating CSPs that contains standard attributes of a CSP and level of concern regarding it. The CSP feedback module submits the collected feedback about CSPs to the CSP Feedback Trust Estimation Engine of the Feedback. It estimates the trust score based on registered CSPs feedback. The Feedback module and SLA module calculates the trust scores based on feedback and SLA mechanisms respectively. All of the calculated trust scores are then passed to the Final Trust Evaluation module. The Final Trust evaluation module evaluates the combined final trust score gained for trustworthiness of CSP.

3.4 Sequence of Operations for Proposed FCTMM

3.4.1 SLA Module

The sequence diagram in figure 3.3 shows the sequence of actions performed in SLA module for trust calculation.

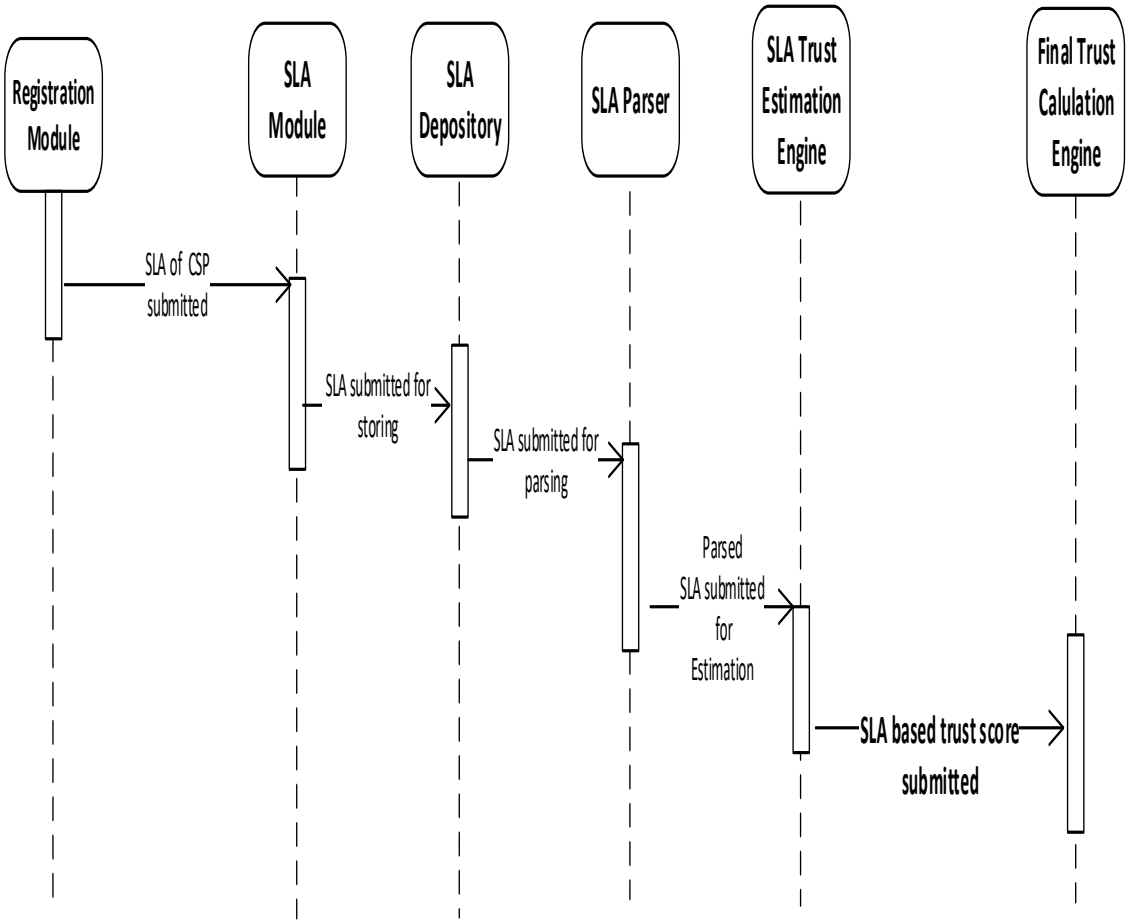

Fig 3.3: sequence Diagram for SLA module

First the Registration Module collects the SLAs of all the registered CSPs. These SLAs are then submitted to SLA depository for storing these SLA's for further use. For the required SLA trust score, the specific SLA moves to the SLA parser for further computation. Finally the parsed SLA moves to the SLA trust Estimation Engine for calculation of final SLA based trust score, this score is then passed to the Trust Management Module.

3.4.2 Customer Feedback Module

The sequence diagram in figure 3.4 shows the sequence of operation for the customer feedback module.

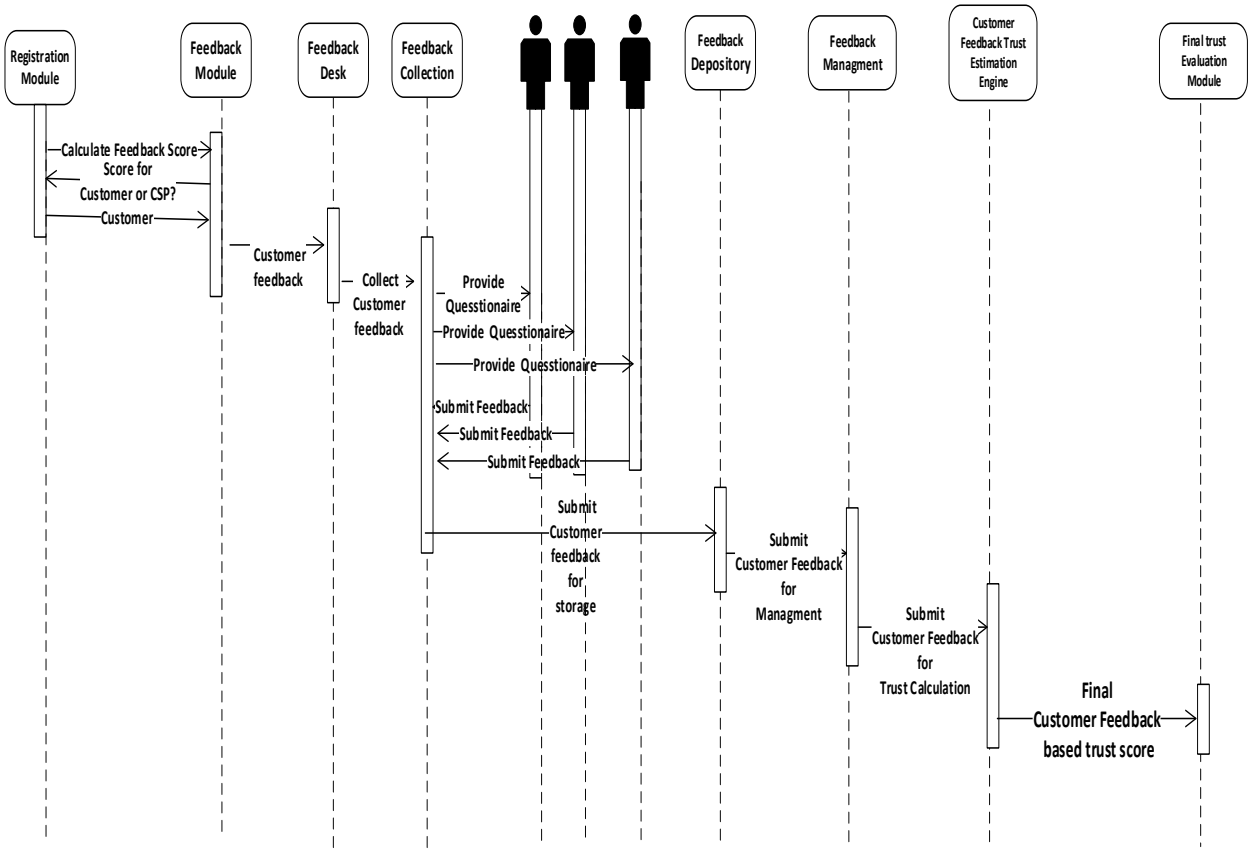

Fig 3.4: Sequence Diagram for Customer feedback module

The actions start with the registration module inquiries about the type of feedback to be submitted. The registration module notify the feedback module about the type of feedback to be submitted which is of the customer. Then this notification is send to the feedback desk which redirects the controls to the feedback collection module. In further processing the feedback collection module provide questionnaire for registered cloud customers. The feedback from the customers is then passed to the feedback collection which submits the collected feedback data to feedback depository for data storage. Further the collected feedback is passed to customer feedback management module which directs it to the customer feedback trust evaluation engine for calculating trust score based on registered customers feedback. The score is calculated and submitted to the final trust evaluation module.

3.4.3 CSP Feedback Module

The sequence diagram in figure 3.5 shows the sequence of actions for CSP feedback module.

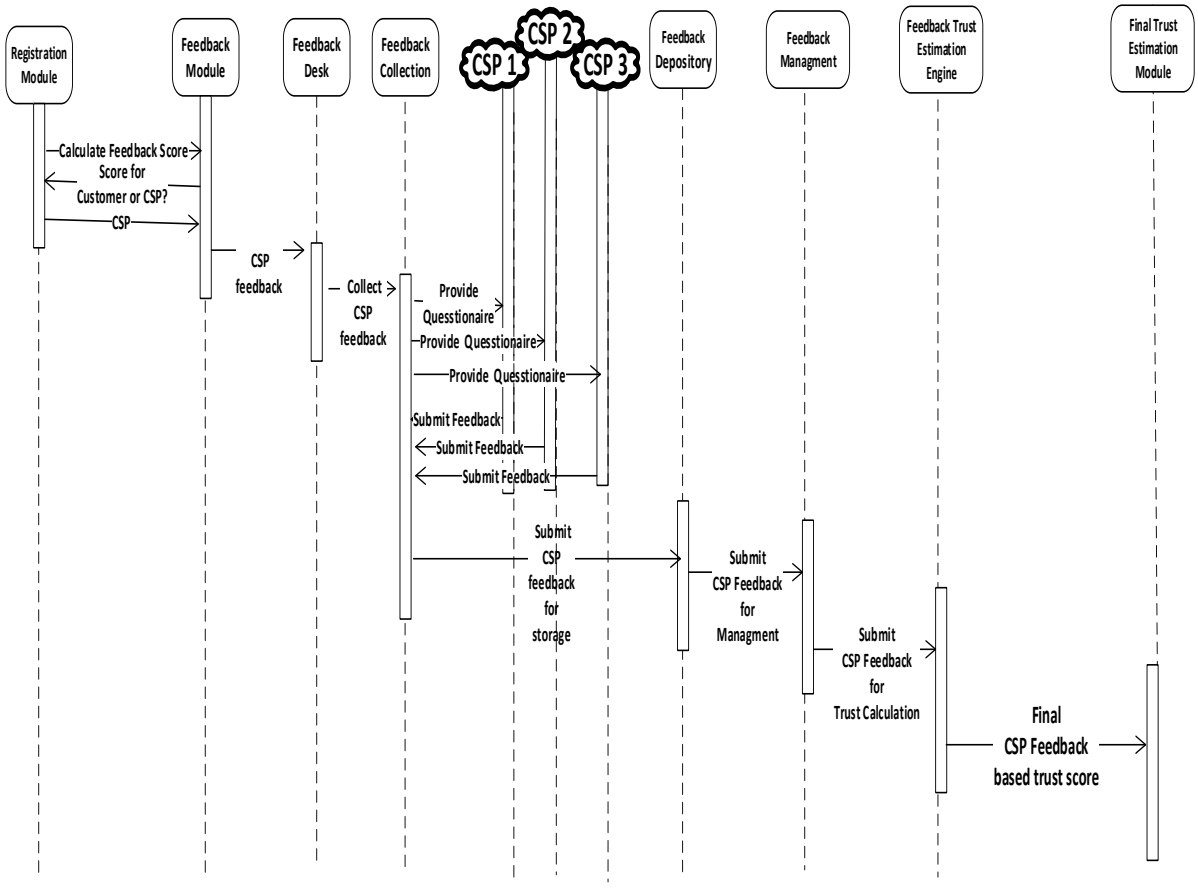

Fig 3.5: Sequence Diagram for CSP feedback module

The process starts with the registration module asks about the type of feedback to be submitted. The registration module notify the feedback module that the type of feedback to be of CSPs. This notification is send by the feedback desk to the feedback collection module. In the next step the feedback collection module provide questionnaire for registered participating CSP's. This feedback is then collected by the collection module and submitted to the CSP feedback depository for storage and further use. It is then passed to CSP feedback management module which pass it on to the CSP feedback trust evaluation engine for trust score based on CSP feedback. The score is calculated and submitted to Final Trust Evaluation Module.

3.4.4 Proposed FCTMM

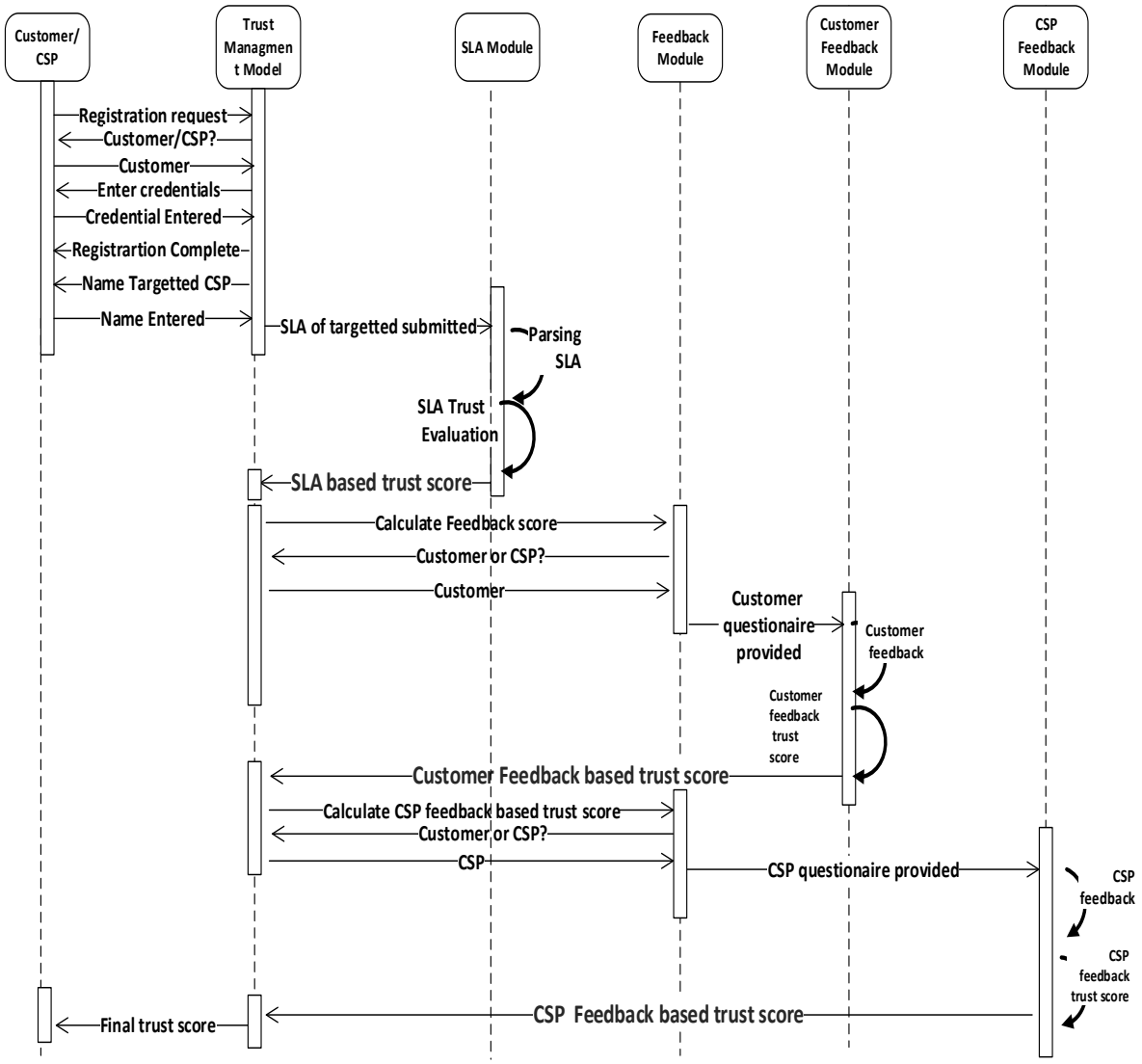

Fig 3.6: Sequence Diagram for Purposed Federated Cloud Trust Management Model

The sequence of actions in figure 3.6 start with the user or CSP to register for the trust management model. The trust management model ask to enter the credentials for registering. After the registration process the model ask for the targeted CSP (Google cloud, Rack space etc.) for trust calculation, after the user or CSP mention the targeted CSP, the control goes to the SLA and feedback module for trust calculation. All the required functions are performed as mentioned in section 3.3.1, 3.3.2 and 3.3.3.The final trust is score is calculated and provided to the user or CSP.

3.5 Components of proposed FCTMM

The architecture of the proposed FCTMM includes Registration Module (RM), Customer Feedback Module (CFM), CSP Feedback Module (CSP-FM) SLA Module (SM) and Final Trust Evaluation Module (FTEM) modules as shown in Figure 3.2. The core functionality of each module is discussed below.

3.5.1 Registration Module

The registration module of proposed FCTMM is accountable for registration of users and CSPs that want to participate in the federated environment. These customers and CSP's are using the services of the cloud service providers. In the registration of customers and CSP's , the registration module collects the SLAs documents of the targeted CSP, which are then used by the SLA Management module for calculation of final SLA based trust score. The registration module also initiates the feedback module for the collection of feedback from customers and CSP's to calculate final feedback based scores.

3.5.2 SLA Module

For many years SLAs have been used in IT organizations as a document for contract. The Service Level Agreement refers to a document or format that defines the explanation of the service that are to be agreed upon, parameters that defines the level of service, the assurance of guarantees regarding the Quality of Service which will be provided, and also includes the compensation in case of violations[34]. The SLA is considered an extremely significant contract that is to be held between the provider of the service and its customers (broker negotiator, or monitoring negotiator).

The description about the qualities like performance, operability, availability and billing method should be mentioned in an SLA. SLA should also include duties and the activities that will be done for providing the required service to its customers. In quantifiable terms the SLA should mention all the services that the cloud service provider will be providing to its customer and an important section must be included that describes that what support the Service Provider will provide in case the mention objectives cannot be met. Some advantages of SLA includes:

1. **Customer acceptance level improvement**:

A good and clear SLA improves the customer approval level, as all the customer needs are focused in it and confirms that the progress is on the right direction.

2. **Building strong relationships between Provider and customer**:

A good SLA describes the payment and payback policies of the service offered. The customer can scrutinize services according to their desire objectives to fit in. Moreover, the SLA must include solutions to solve contractual disagreements without difficulty.

3. **Improve Quality of service:**

Key Performance Indicators (KPI) that are included in an SLA, determines the customer service by tracking whether or not the mentioned indicators match the requirements between customers and service providers. This clarifies all the quality parameters and help improve the service.

a) Generic components of SLA

Figure 3.8 shows the major components of SLA. The details of the components are mentioned below:

Fig 3.8: SLA components

1. **Purpose**: explains the reasons to form an SLA.
2. **Parties:** states about all the participating parties that are included in the SLA contract and give brief description of their jobs.
3. **Validity Period**: brief about the duration of the SLA. Both the start time and the final time of the SLA formation is mentioned here.
4. **Scope**: defines all the services provided by the service provider in the SLA. SLA must clarify the services that are to be provided so that the consumer can easily recognize all the services procedures of the desired service provider.
5. **Restrictions**: briefly explains all the important tasks or procedures to be done in order to get the required level of services.
6. **Service-level objectives**: mentions all the service levels that are accepted by the customer and the required service providers. It includes indicators such as; availability, performance, and reliability, each indicator is explained properly and parameters are defined clearly.
7. **Service-level indicators**: these are indicators that are used to measure the quality of service provided by service providers.
8. **Penalties**: defines the compensations to be done when the service provider is not able to achieve the desired goals set in the SLA
9. **Optional services**: mentions the services that are not necessarily needed by the customer for service, but they might be needing them as exclusion.

- **Generic SLA Parameters**

SLA contains different parameters that define the quality of service that they provide .It can also be used by the customers as an easy and quick way for comparison between different service providers to choose the most suitable and best among them[4][30]. Iaas service models for accessing, monitoring, and managing remote datacenter infrastructures. Table 3.1 shows the standard parameters of Iaas platform along with the description.

Table 3.1: Standard SLA parameters for Iaas platform

S. No.	Parameter	Description
1	**CPU capacity**	Is the ability and speed of a virtual machine, and describes in a given amount of time how many operations it can carry out.
2	**Memory size**	Cache memory capacity of virtual machine
3	**Boot time**	The time taken the virtual machine to get ready for operate after it is turned on
4	**Storage**	Storage capacity of data for the total contractual time
5	**Scale up**	Maximum amount of virtual machines per user
6	**Scale down**	Minimum amount of virtual machines provided per user
7	**Scale up time**	Time taken to increase the number of Virtual machines
8	**Scale down time**	Time taken to decrease the number of Virtual machines
9	**Availability**	Specific time for service uptime
10	**Response time**	Time to complete the process

Paas platform is a framework used to develop or customize applications. Paas eases development, testing of applications which prove to be very cost-effective. Table 3.2 shows the standard parameters of Paas platform along with the description.

Table 3.2: Standard SLA parameters for Paas platform

S. No.	Parameter	Description
1	**Integration**	Capability to integrate with other platforms.
2	**Scalability**	Ability to add new components without disturbing the system.
3	**Pay as you go billing**	Charge as per use.
4	**Environments of deployment**	Offline support availability.
5	**Browsers**	Chrome , Firefox, Explorer etc.
6	**Number of developers**	Total no of developers that have access to platform.

Saas platform is growing quickly. It uses the internet services to deliver applications that are managed by a third-party. Table 3.3 shows the standard parameters of Saas platform along with the description.

Table 3.3: Standard SLA parameters for Saas platform

S. No.	Parameter	Description
1	**Reliability**	Guarantee of operation under different circumstances
2	**Usability**	Easy to understand user interface
3	**Scalability**	Ability to expand or contract modules as per requirement
4	**Availability**	Users uptime
5	**Customizability**	Ability to show flexibility for ease of use

- **Components of proposed SLA module**

Figure 3.9 shows the components of proposed SLA module. The details of each component is discussed below:

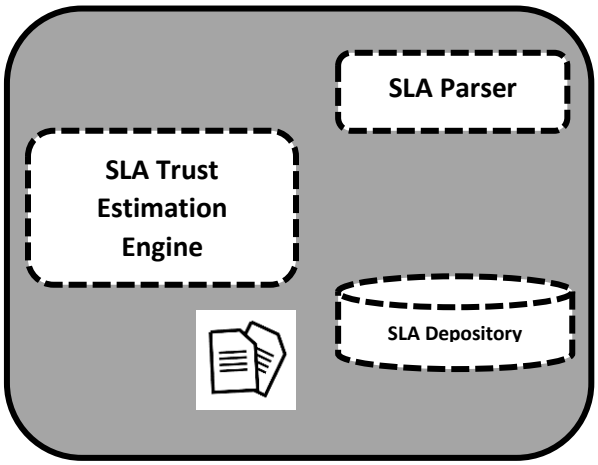

Fig 3.9: Components of SLA module

a) SLA Depository

This is the first component in SLA mechanism. The SLA depository collects the SLA's from the registered CSP and store them. The SLA's of individual CSP's is saved using their identity number, name and URL to differentiate them from each other. These SLA's are then passed on to the SLA parser for further evaluation.

b) SLA Parser

The second component is SLA parser. After storing the SLA's the SLA depository passed it on to SLA parser. SLA Parsing is the task of this module hence it is named after its function. As it receives the SLA from the SLA depository it locates and gathers the essential security and privacy parameters included in the SLA of the targeted CSP. This module especially searches for the compulsory standard parameters in SLA which must be provided by the CSP to increase its level of trust. To give an idea about SLA parameter evaluation, summary of SLA parameters of several CSP is provided in the table below.

Table 3.4: Summary of SLA parameters of several CSP

Cloud Provider / SLA parameter	Amazon	Microsoft Azure	Rack space	Google cloud storage
Type of service	Iaas	Paas	Iaas	Paas
Service Availability	99.5%	99.9%	99.9%	99.9%
SLA outlining [23]	Predefined terms and QoS parameters[23]	Predefined terms and QoS parameters	Predefined terms	Predefined terms and QoS parameters
Establishment of Agreement [23]	SLA document provisioned by the provider	SLA document provisioned by the provider	SLA document provisioned by the provider	SLA document provisioned by the provider
Data backup and recovery	Provide backup and recovery	Provide backup and recovery	Provide backup and recovery	Provide backup and recovery
Encrypted Storage	Do not provided the service	Provide the service	Do not provided the service	Do not provided the service
Access Control	Provide the service	Provide the service	Provide the service	Provide the service
Authentication	Provide the service	Provide the service	Provide the service	Provide the service

c) SLA Trust Estimation Engine

This is the third most important component of SLA module .In this component the extracted security and privacy parameters from SLA parser are passed on to the SLA based Trust Estimation Engine for final calculation of SLA based trust score. The security and privacy parameters that are considered includes confidentiality, integrity , authentication, access control, data backup and recovery ,encrypted storage , availability and frequent SLA updates.

The data of parameters are represented by the set ***P={C, In, Auth, Ac BnR, Es, Av, Sap}*.** Scales are assigned to these parameters according to the impact on the system as a whole including availability of these parameters in the SLA document. The scaling is as follows:

- **Critical (0.9):**

A critical scale applies to vulnerabilities that will interrupt the system completely and a complete system compromise will occur along with easy exploitation.

- **Medium (0.8):**

A medium scale applies to vulnerabilities that will not interrupt system as a whole but have a huge impact on security concerns of system.

- **Low (0.7):**

This scale applies to vulnerabilities that depends on unlikely situations in order to interrupt the system. These situations include a flawed or unlikely configuration of the system be in place.

The SLA based trust score S_{SLA} is calculated using equation 3.1

$$\boldsymbol{S_{SLA}} = \frac{\sum_{i=0}^{n}(L_i * SP_i)+(m*\tau)}{|Np|} \quad \textbf{(}3.1\textbf{)}$$

Where margin of error $\boldsymbol{m}$ is calculated using equation 3.2

Margin of Error

$$\boldsymbol{m} = \frac{N_l}{N_p+N_l} \quad (3.2)$$

$\boldsymbol{\tau}$ defines the Threshold for evaluation of trust which is calculated using equation 3.3

Threshold $\boldsymbol{\tau} = 1/N_l$ (3.3)

$\boldsymbol{N_l}$ represents the total no of levels defined for scaling purpose. $\boldsymbol{N_p}$ is total no of parameters that are taken as standard features of security and pivacy concerns.$\boldsymbol{L_i}$ represnts the Level assigned to each parameter accordingly. $\boldsymbol{SP_i}$ is the ith Security Parameter that is taken.

3.5.3 Feedback Module

Feedback is considered important for learning and assessment purpose. Feedback allows the user to estimate different parameters in a systematic way [35]. Suppose a user of a CSP by giving feedback can give opinion about the security and privacy concerns. It

can also considered as a freedom of expression. This not only helps the user but also helps the CSP to estimate its market value. By evaluating the feedback provided by the user, the CSP can compare its worth among other competitors and pin point its weaknesses and have a grip on its strength .This proves to be a very successful methodology as CSP overcome its weakness it can increase the customers and strengthen the CSP economically. There are different types of feedbacks mentioned in the figure 3.10 below.

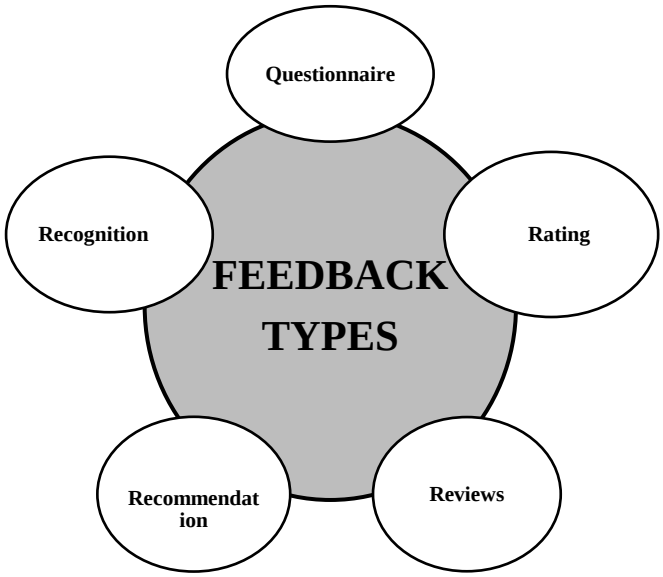

Fig 3.10: Types of feedback

a) Questionnaire (Customer, CSP)

In this type of feedback the customer is provided with several questions about the services provided by the CSP. The questions covered include security, privacy, availability, operability and other important concerns.

b) Reviews (Customer ,Management, Peer, Audit)

Review is a type of feedback which no question is asked but the customer describes the CSP services in descriptive form.

c) Rating

In this form the customer rate the CSP, rating is based on different criteria's. One example is the number of services provided by a certain CSP. The customer can rate it in number (1-5) or leave star (1-5).

d) Recommendation

Recommendation is done on the basis of experience by the customer. If the customer experience with a particular CSP is good enough the customer recommend the CSP to others for use. It adds value the particular CSP.

e) Recognition

If number of user recognize a CSP and uses it also provides a glimpse about the quality and reflects that good service is provided by the CSP.

3.5.4 Customer Feedback Module

Figure 3.11 shows the customer feedback module and its component. It collects all the responses from the registered customers. It includes the following components.

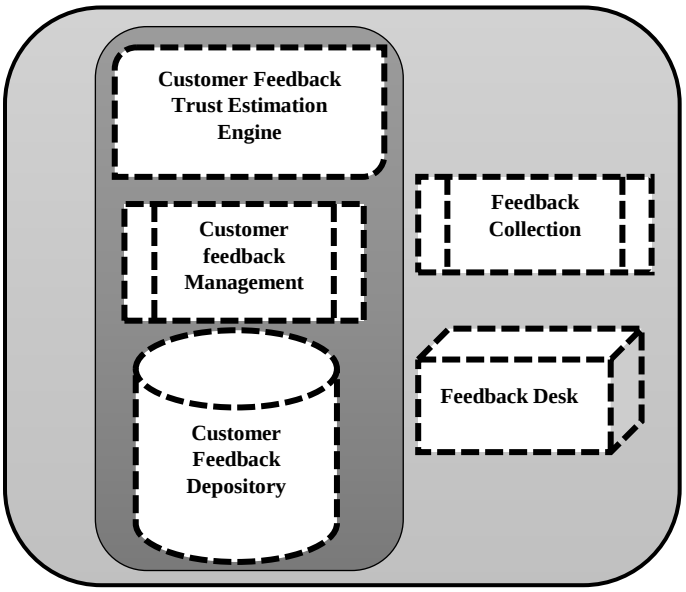

Fig 3.11: Components of Customer Feedback module

a) Feedback Desk

Feedback desk first informs and directs the customer/ CSP about the type of feedback to be filled in. If the feedback is from the customer it directs it to the customer feedback mechanism and if it's from CSP it shifts the control to CSP feedback mechanism.

b) Feedback Collection

The task of Feedback Collection module is to collect the feedback regarding security and privacy parameters available by the targeted CSPs. For the customer feedback the process is to collect it in the form of a provided questionnaire which is filled by the

registered customers. The questionnaire provided contains 30 questions to be answered according to the individual experience.

- **Customer Feedback Depository**

The function of customer feedback module is to collect the submitted feedback from the customer by the Feedback Collection Module. This module also stores the basic information of the customers.

- **Customer Feedback Management**

The customer feedback management module performs the management of the storage of the user feedback at backend database. All the feedback which is collected is then passed on to the user feedback estimation engine for trust evaluation.

- **Customer Feedback Trust Estimation Engine**

The Customer Feedback based Trust Estimation engine collects the feedback of the registered customers from the customer feedback management module and calculates the final trust score of this module. Mathematical logic is applied for the calculation of final user feedback based trust score [21].The trust score is calculated based on different options provided by the module and the respective customer responses. Here p_r is the positive response calculated using equation 3.5, n_r is calculated using equation 3.6, it represents the negative response and U_r relates to uncertain response given by the customer for the targeted CSP represented as CSP and is calculated equation 3.7. Total trust score of individual customer is T_{csp}^{C} which is calculated using equation 3.4, whereas N represents the total number of customers giving responses about the targeted CSP. Individual trust score by the customer is calculated using equation 3.8.

$$\boldsymbol{T_{csp}^{C} = (p_r, n_r, U_r, m, \tau)} \tag{3.4}$$

$$\boldsymbol{p_r = \frac{positive\ response}{collected\ response + N_s}} \tag{3.5}$$

$$\boldsymbol{n_r = \frac{negative\ response}{collected\ response + N_s}} \tag{3.6}$$

$$\boldsymbol{U_r = \frac{uncertain\ response}{collected\ response + N_s}} \tag{3.7}$$

$$T_{csp}^{C\,1}\ , T_{csp}^{C\,2}, T_{csp}^{C\,3}, \ldots . T_{csp}^{C\,N} \tag{3.8}$$

Here m represents the margin of error calculated using equation 3.9

$$\boldsymbol{m} = \frac{N_s}{collected\ response + N_s} \tag{3.9}$$

τ is the threshold value

$$\boldsymbol{\tau = 1/N_s} \tag{3.10}$$

$\boldsymbol{N_s}$ Defines the total no of scales defined for a user to give responses. After calculating the individual customer trust score on a CSP from equation 3.4, the overall trust score of a CSP is calculated by combining all the responses from all the customers this is shown by the equation 3.11. 3.12, 3.13, 3.14, 3.15 as follows.

$$T_{csp}^{C\,1} + T_{csp}^{C\,2} = (p_{new}, n_{new}, u_{new}, m_{new}, b_{new}) \tag{3.11}$$

$$p_{r_{new}} = \frac{(p_{r_{csp}}^{C\,1} + m_{csp}^{C\,2}) + (p_{r_{csp}}^{C\,2} * m_{csp}^{C\,1})}{m_{csp}^{C\,1} + m_{csp}^{C\,2} - m_{csp}^{C\,1} * m_{csp}^{C\,2}} \tag{3.12}$$

$$n_{r_{new}} = \frac{(n_{r_{csp}}^{C\,1} + m_{csp}^{C\,2}) + (n_{r_{csp}}^{C\,2} * m_{csp}^{C\,1})}{m_{csp}^{C\,1} + m_{csp}^{C\,2} - m_{csp}^{C\,1} * m_{csp}^{C\,2}} \tag{3.13}$$

$$U_{r}^{}new = \frac{(U_{r_{csp}}^{C\,1} + m_{csp}^{C\,2}) + (U_{r_{csp}}^{C\,2} * m_{csp}^{C\,1})}{m_{csp}^{C\,1} + m_{csp}^{C\,2} - m_{csp}^{C\,1} * m_{csp}^{C\,2}} \tag{3.14}$$

$$m_{new} = \frac{(m_{csp}^{C\,1} * m_{csp}^{C\,2})}{m_{csp}^{C\,1} + m_{csp}^{C\,2} - m_{csp}^{C\,1} * m_{csp}^{C\,2}} \tag{3.15}$$

Trust score given by individual customer is combined with the trust score provided by other customers. This operation is executed iteratively until final trust score is achieved. The expected score of trust of a CSP by individual customer is calculated using equation 3.16,

$$S_e = p_{r_i} + m_i * \tau_i \tag{3.16}$$

Where p_{r_i} is the positive response of a customer and $m_i\ and\ \tau_i$ are the margin of error and threshold values respectively.

3.5.5 Cloud Feedback Module

Figure 3.12 shows the cloud feedback module and its component. It collects all the responses from the registered CSP's. It includes the following components.

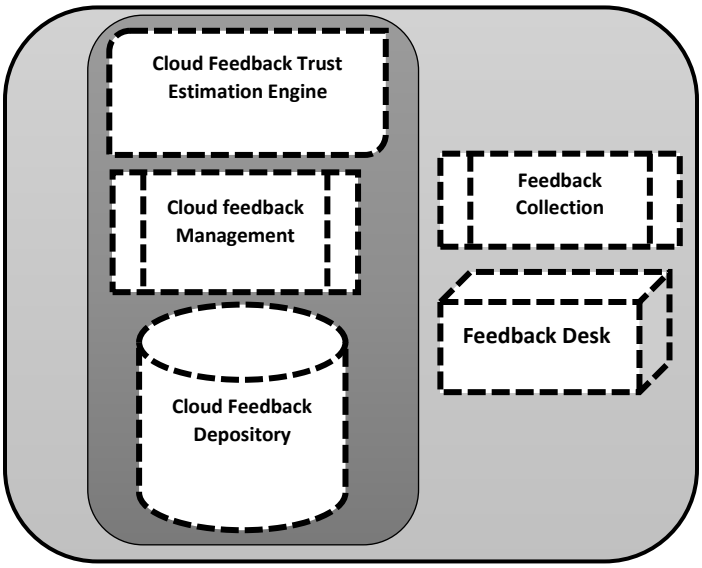

Fig 3.12: Components of CSP Feedback module

a) Feedback Desk

Feedback desk first informs and directs the customer/ CSP about the type of feedback to be filled in. If the feedback is from the customer it directs it to the customer feedback mechanism and if it's from CSP it shifts the control to CSP feedback mechanism.

b) Feedback Collection

The task of Feedback Collection module is the collection of feedback regarding security and privacy parameters available s by CSPs. For the CSP's feedback mechanism the feedback is collected by concerned CSP's about the individual target CSP in the form of a questionnaire. It includes different standard attributes about a CSP and the registered CSP's rate it according to their Level of concern regarding each attribute. The concern are categorized into three levels high, moderate and low which are marked according to the target CSP performance.

a) Cloud Feedback Depository

The function of cloud feedback module is to collect the submitted feedback from the registered CSP's by the Feedback Collection Module. This module also stores the basic information of the CSP's.

b) Cloud Feedback Management

The cloud feedback management module performs the management of the storage of the cloud feedback at backend database. All the feedback which is collected is then passed on to the cloud feedback estimation engine for the final trust evaluation score.

c) Cloud Feedback Trust Estimation Engine

The cloud Feedback based Trust Estimation engine collects the feedback of the registered CSP's from the cloud feedback management module and calculates the final trust score of this module. Mathematical logic is applied for the calculation of final cloud based feedback trust score. The feedback is based on responses of several registered peer clouds that are using the services of the targeted cloud [35]. Every peer CSP gave an opinion about the respective CSP about certain standard features that are defined in the provided questionnaire. Against these standard features peers have to give responses The total score of the defined feature marked by all participating peers $\mathbf{T}_f$ evaluated by the following formula 3.17.

$$\mathbf{T}_f = \sum_i^{\boldsymbol{T_{peer}}} \frac{(W_i * peer_i)}{peer_i} \qquad (3.17)$$

Where W_i is the weight given by module according to a specific criteria, $peer_i$ and represents the individual Score given by peer clouds participating in evaluating trust. Total Trust score for cloud feedback estimation Engine $\mathbf{S}_{\boldsymbol{CLOUD}}$ is calculated using the following equation 3.18 as follows:

$$\mathbf{S}_{\boldsymbol{CLOUD}} = \left[\frac{\sum_{i=0}^{F_T} \mathbf{T}_f}{|\boldsymbol{T_{peer}}|}\right] * (\boldsymbol{m} * \boldsymbol{\tau}) \qquad (3.18)$$

Where F_T is the total no. of features defines in the questionaire. Total numbers of levels defined for giving response is N_l and T_{peer} represents the total no of peers participating in evaluation of trust.

Margin of error m and threshold value τ is calculated using equation 3.19 and 3.20,

$$\boldsymbol{m = \frac{N_l}{T_{peer}+N_l}} \quad (3.19)$$

$$\boldsymbol{\tau = 1/N_l} \quad (3.20)$$

3.5.6 Final Trust Evaluation

The Final Trust Evaluation module is responsible for the collection of the evaluated trust scores .It combines all of the trust values and calculates an aggregated final trust score $\boldsymbol{T_{SCORE}}$ of the targeted CSP is calculated using equation 3.21 as follows.

$$\boldsymbol{T_{SCORE} = \frac{S_{SLA} + S_e + S_{Cloud}}{3}} \quad (3.21)$$

Where S_{SLA} , S_e and S_{CLOUD} represents trust scores from SLA trust estimation engine and Customer trust estimation engine and cloud trust estimation engine respectively. The range of trust is also determined in Final trust evaluation module by using the table below. This will help in determination of CSP trustworthiness by evaluating the range and level of trust the CSP gained. After the final trust score the module also indicates the range of trust accordingly. The table 3.5 below shows the range of trust a CSP gained using FCTMM.

Table 3.5: Defined range of trust

Final trust score range	**Range of trust**	**Level of trust**
0 < T_{SCORE} < 0.2	ROT 1	**LOW**
0.2 < T_{SCORE} < 0.4	ROT 2	
0.4 < T_{SCORE} < 0.6	ROT 3	**MEDIUM**
0.6 < T_{SCORE} < 0.8	ROT 4	**HIGH**

3.6 Conclusion

In this chapter a new cloud trust federation model for CSP's named FCTMM has been presented. As it has been quite elaborated, FCTMM provides all the security provisions for users, CSP's. In the next chapter the practical implementation and results of the proposed FCTMM will be discussed and the model will be analyzed and compared for the compliance with other existing trust model.

Chapter 4

IMPLEMENTATION AND RESULTS

4.1 Introduction

This chapter constitutes the details of our proposed FCTMM for Evaluation and Establishment of Trust in Cloud Computing. This model helps to evaluate trust of the CSP's in a reliable and trusted way. The proposed FCTMM is based on three modules for the process of trust evaluation which are SLA module, feedback from customer's module and feedback from clouds**.** For the SLA module parameters that are in security and privacy domains are extracted by SLA parsing. A total trust score is calculated using separate trust scores obtain from these proposed mechanisms. The chapter also provides the details of implementation and the results obtained from them.

4.2 Experimental Setup

The proposed FCTMM is implemented in Java J2EE Eclipse [37]. For complete database storage MySQL is used. For the experimental setup three cloud setup is formed on Linux machines using open source cloud OpenStack. Federated Cloud Trust Management system is deployed on one cloud and two other participating CSP's are deployed on the other two cloud setups. All the three Clouds are communicating via SAML v2.0 protocol for communication [38].

First Tomcat server is installed on Windows. Then Environment variable for Tomcat server is set accordingly. The next step is the installation of MySQL Database Server. The setup is easily available on its website. Then all the project files are compiled and the site is run, it will be open in browser and can be logged in with the desired username and password.

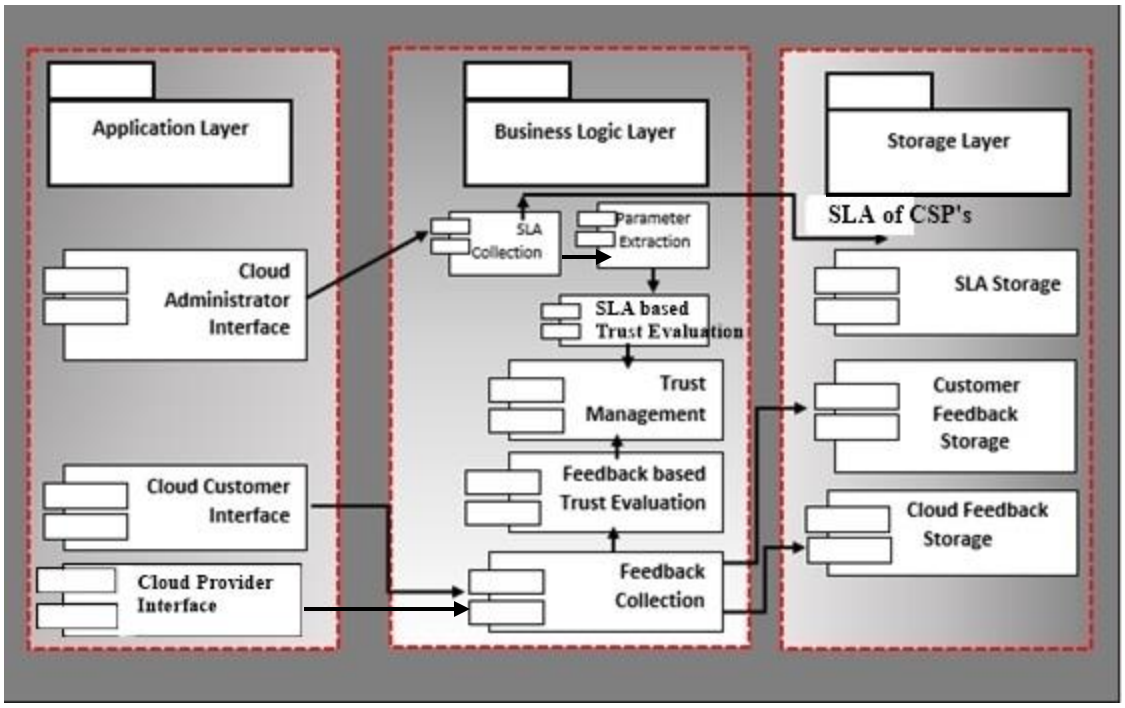

Fig 4.1: Component Diagram of Federated Cloud Trust Management System

The interaction with different components of FCTMM is illustrated in figure 4.1. The figure illustrates that there are three basic layers of the purposed FCTMM. These layers include application layer, business logic layer and storage layer. The application layer consists of cloud administrator interface which directly links to SLA collection component in the business logic layer. The cloud customer interface and the cloud provider interface collects the feedback from the registered customers and CSP's and sends it directly to the feedback collection component in business logic layer. The business logic layer consists of several components as feedback collection, feedback based trust evaluation, trust management, SLA collection and parameter extraction. All these components contribute towards the final trust evaluation. The third is the storage layer which store all the SLA's of CSP's and the feedback collected from registered customers and clouds.

4.2 Implementation of Proposed FCTMM

The figure 4.2 shows the series of operations that are performed during federation establishment between two CSP's. The procedure for the proposed FCTMM is presented in detail.

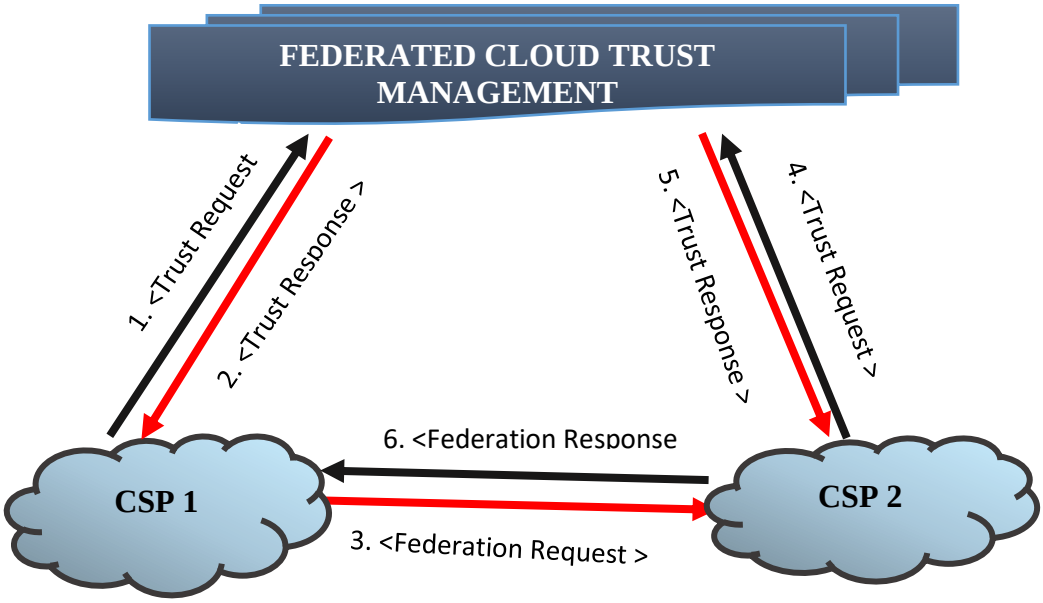

Fig 4.2: Workflow of FCTMM

The two participating CSPs need to establish a trusted environment between them so they could built a trusted federation to share their available resources to get maximum benefit. The presented protocol is based on Trust Score, Level of trust and Range of Trust to establish federation. Security Assertion Markup Language (SAML) is used for the presented FCTMM which is an XML-based standard to support the security parameters like authentication and authorization decisions [27]. A new type of assertion is introduced in SAML that satisfies the extension mechanism [27] for compatibility assurance. The assertion used contains Trust Statement (TST) which includes four type of trust attributes that are SLA of targeted CSP, over all TrustScore and LevelOfTrust (LOT) and RangeOfTrust (ROT) for the participating CSPs.

The Trust statement starts with mentioning the <Issuer> tag that is the FCTMM while the tag <Subject> here is used for the CSP which requested the trust attributes. Here the trust statement includes attributes that are mainly TrustScore (TS) which contains the accumulated trust value, LOT that contains the assigned LOT value to the CSP, ROT that contains that range of trust between medium, low or high and the SLA of the CSP.

The proposed FCTMM acts as a trusted third party which holds the responsibility to provide the requested trust statements about participating CSPs. The proposed model

receives the TrustRequest (TRQ) from one CSP and in response to that it generates the TrustResponse (TRS) that contains the asserted trust attributes for the other CSPs as depicted in figure above. The main steps involved in trust establishment using our proposed protocol are discussed below.

STEP 1:

The mechanism starts when CSP who wants to establish a trusted federation sends a TRQ to the FCTMM and requests for the trust attributes of the targeted CSP. For the above scenario CSP1 is the Trust Requestor.

```
<samlp: TrustRequest
<saml: Issuer> CSP1
</saml: Issuer>
<saml: Subject>
CSP2
<saml:NmaeID
Format =”urn:oasis:names:tc:SAML:2.0:NameID-format: url">
www.CSP1.com
</saml:NameID>
</saml: Subject>
   <samlp:RequestedTrustRequest>
   <saml:TrustContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:Classes:ServiceLevelAgreement
</saml:TrustContextClassRef>
      <saml:TrustContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:Classes:Feedbackfromusers
</saml:TrustContextClassRef>
     <saml:TrustContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:Classes:FeedbackfromCSPs
</saml:TrustContextClassRef>
      <saml:TrustContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:Classes: ServiceLevelAgreementwithFeedback
     </saml:TrustContextClassRef>
   </samlp: RequestedTrustContext>
</samlp:TrustRequest>
     <saml: resourse
SLA of CSP2
     </saml: resourse>
<saml: action
Read
</saml: action>
```

```
  <saml:resourse
SLA of CSP1
</saml:resourse>
  <saml:action
Read
</saml:action>
```

STEP 2:

The FCTMM authenticates the request from CSP1 and the function moves to the proposed modules namely SLA extraction, Feedback from customers and feedback from peer CSP's for evaluation of trust attributes. The requested trust score for CSP2 is calculated .After evaluating the trust attributes, FCTMM sends a **TRS** containing the **TST** for CSP2. The **subject** of this statement is CSP2 whereas FCTMM is the Issuer of the assertion. The FCTMM is the Trust Responder.

```
<saml:TrustResponse>
  <saml:Truststatement>
    <saml:TrustContext>
       <saml:TrustContextClassRef>
ServiceLevelAgreement
       </saml:TrustContextClassRef>
    <saml:TrustContextClassRef>
Feedbackfromusers
</saml:TrustContextClassRef>
  <saml:TrustContextClassRef>
FeedbackfromCSPs
  </saml:TrustContextClassRef>
  <saml:TrustContextClassRef>
ServiceLevelAgreementwithFeedback
  </saml:TrustContextClassRef>
    </saml:TrustContext>
  <saml:SLATrustScore> 0.5613
  </saml:SLATrustScore>
     </samlp:TrustResponse>
  <saml:FeedbackfromusersTrustScore> 0.453
 </saml:FeedbackfromusersTrustScore>
  <saml:FeedbackfromCSPsTrustScore> 0.565
 </saml:FeedbackfromCSPsTrustScore>
    <saml:ServiceLevelAgreementwithFeedbackTrustScore> 0.5263
   </saml:ServiceLevelAgreementwithFeedbackTrustScore>
  <saml:RangeofTrust> ROT3
 </saml:RangeofTrust>
<saml:LevelofTrust> Medium
</saml:LevelofTrust>
<Resource type>
//XML Service Level Agreement document CSP2
<Resource type>
</saml:TrustStatement>
</saml:Assertion>
</samlp:TrustResponse>
```

STEP 3:

Then the TRS is extracted by CSP1and all the trust attributed are read from it. Then it compares the provided TS with its own accepted trust threshold. If the provided Trust attributes value is greater than the required threshold value then a FRQ is forwarded to the

targeted CSP2 by CSP1. On the other hand if the TS is less than the required threshold then CSP1 searches for another CSP to establish trusted federation.

```
<fedp:FederationRequest>
  <fedp:Issuer> CSP1
</fedp:Issuer>
  <ResourseType>
" XML Federation Resource"
  </ResourseType>
</fedp:FederationRequest>
```

STEP 4:

Another operation is performed before sending response to the received FRQ, in this regard the targeted CSP2 also wants to calculate the trustworthiness of CSP1. In this regard, CSP2 generates a TRQ for trust attributes of **CSP1**and sends this request to the Federated Cloud Trust Management Model. In this step, the CSP2 becomes the Trust Requestor**.**

```
  <samlp:TrustRequest
 <saml:Issuer> CSP2
</saml:Issuer>
 <saml:Subject>
CSP1
  <saml:NameID
Format ="urn:oasis:names:tc:SAML:2.0:NameID-format: url">
www.CSP2.com
 </saml:NameID>
</saml: Subject>
  <samlp:RequestedTrustRequest>
     <saml:TrustContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:Classes:ServiceLevelAgreement
     </saml:TrustContextClassRef>
   <saml:TrustContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:Classes:Feedbackfromusers
   </saml:TrustContextClassRef>
 <saml:TrustContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:Classes:FeedbackfromCSPs
 </saml:TrustContextClassRef>
  <saml:TrustContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:Classes: ServiceLevelAgreementwithFeedback
   </saml:TrustContextClassRef>
  </samlp:RequestedTrustContext>
</samlp:TrustRequest>
```

STEP 5:

Then the FCTMM receives the request from CSP2 and confirms this request. The FCTMM calculates the trust score and LOT and ROT for CSP1. TEM then generates the SAML <TrustResponse> that contains the TST for CSP1 **(**TrustScore**,** SLA, ROT and LOT

of CSP1). Here the FCTMM acts as a Trust Responder**,** and sends the encrypted assertion to CSP2. The <Subject> of this response is the CSP1 whereas FCTMM is the <Issuer> of the assertion.

```
<saml:TrustResponse>
  <saml:Truststatement>
   <saml:TrustContext>
     <saml:TrustContextClassRef>
ServiceLevelAgreement
    </saml:TrustContextClassRef>
   <saml:TrustContextClassRef>
Feedbackfromusers
   </saml:TrustContextClassRef>
   <saml:TrustContextClassRef>
FeedbackfromCSPs
   </saml:TrustContextClassRef>
   <saml:TrustContextClassRef>
ServiceLevelAgreementwithFeedback
  </saml:TrustContextClassRef>
```

STEP 6:

In the last step CSP2 extracts the trust attributes after verifying the assertion and compares their values with its own pre-defined acceptable trust threshold values. If the trust value of CSP1 is satisfactory then CSP2 generates a federation response to accept the request or a corresponding rejection message in case of low TrustScore.

IN CASE OF ACCEPTING

```
<samlp:Response
  <Issuer CSP2
</Issuer>
  <samlp:Status>
 <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Federation Accepted" />
  </samlp:Status>
</samlp:Response>
```

IN CASE OF REJECTION

```
<samlp:Response
  <Issuer CSP2
</Issuer>
  <samlp:Status>
 <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Federation Rejected" />
  </samlp:Status>
</samlp:Response>
```

4.3 Results and discussion

The results fabricated by using the above policies implemented in SAML for the proposed FCTMM are discussed in table 4.1 below.

Table 4.1: SLA based Trust module results

Standard Parameters	**Extracted Parameters**	**Parameters of set S**	$\sum(L_i * SP_i)$	**Final SLA based score**
Confidentiality	SLA contains Confidentiality	0.9	(1*0.9)	$S_{SLA} = \frac{\sum_{i=0}^{n}(L_i * SP_i) + (m * \tau)}{\|Np\|}$ = ((1*0.7) +(0*0.8)+ (1*0.9) + (1*0.9)+(1*0.9)+ (0*0.8)+(1*0.9)+(0*0.7)) *(0.2*0.33) /(8) = 0.56135
Integrity	**Does not** contain Integrity	0.8	(0*0.8)+ (1*0.9)	
Authentication	SLA contains Authentication	0.7	(1*0.7) +(0*0.8)+ (1*0.9)	
Access Control	SLA contains Access Control	0.9	(1*0.7) +(0*0.8)+ (1*0.9) + (1*0.9)	
Data backup and recovery	SLA contains Data backup and recovery	0.9	(1*0.7) +(0*0.8)+ (1*0.9) + (1*0.9)+(1*0.9)	
Encrypted Storage	**Does not** contain Encrypted Storage	0.8	(1*0.7) +(0*0.8)+ (1*0.9) + (1*0.9)+(1*0.9)+ (0*0.8)	
Availability	SLA contains Availability	0.9	(1*0.7) +(0*0.8)+ (1*0.9) + (1*0.9)+(1*0.9)+ (0*0.8)+(1*0.9)	
SLA updates	**Does not** contain SLA updates	0.7	(1*0.7) +(0*0.8)+ (1*0.9) + (1*0.9)+(1*0.9)+ (0*0.8)+(1*0.9)+(0*0.7)	

The table 4.1 shows results for Trust score obtained from SLA based mechanism. First total of eight parameters are identified. The SLA parser module do not found Integrity encrypted data and proper SLA updates. The weights allocated by the model are applied to these extracted parameters accordingly as high (0.9) moderate (0.8) or low (0.7). Then the final SLA score $\mathbf{S}_{SLA}$ is calculated and shown in last column of the table.

Table 4.2 shows the results for user feedback based module for the evaluation trusted CSP. We consider six different registered users for user based feedback module. The user submitted their feedback through a questionnaire provided by the enrolment module. This questionnaire consist total of thirty questions regarding the security and privacy considerations about the targeted CSP. Third, fourth and fifth columns of table represent the positive, negative and uncertain feedbacks submitted by users. Trust

estimation vectors are calculated for each individual user. Then combined cumulative trust scores are calculated by adding the resultant of first two individual trust vectors with the next user trust vector and so on. Then the final trust scoreS_{u1}, S_{u2}, S_{u3}, and S_{u4} denotes the final trust scores for each cumulative trust score for each step. Finally S_{u5} is the Final trust score for resultant of all cumulative scores and it represents the feedback based trust score for the user feedback module.

Table 4.2: User feedback based Trust module results

Registered Users	Total Questions	Positive feedback	Negative feedback	Uncertain feedback	Trust Vector $T_{csp}^{C} = (p_f, n_f, U_f, m, \tau)$	Cumulative Trust Score	Final Trust Score
User 1	30	15	5	10	T_{csp}^{C1} =(0.454, 0.151, 0.303 ,0.090 ,0.333)	----------	--------
User 2	30	15	13	2	T_{csp}^{C2} =(0.454, 0.393, 0.060, 0.090, 0.333)	$T_{csp}^{C1} + T_{csp}^{C2}$ = ($p_{f_{new}}, n_{f_{new}}, U_{f_{new}}, m, \tau_r$ (0.476,0.285, 0.190,0.047,0.333)	S_{u_1} = 0.492
User 3	30	7	10	13	T_{csp}^{C3} =(0.393,0.303,0.212,0.090, 0.333)	Resultant + T_{csp}^{C3} (0.462,0.301,0.204, 0.032, 0.333)	S_{u_2} = 0.473
User 4	30	19	2	9	$_{csp}^{C4}$ =(0.575,0.060,0.272,0.090, 0.333)	Resultant + T_{csp}^{C4} (0.504,0.243,0.227, 0.0243,0.333)	S_{u_3} = 0.512
User 5	30	3	17	10	T_{csp}^{C5} =(0.303,0.515, 0.090,0.090,0.333)	Resultant + T_{csp}^{C5} (0.470,0.307, 0.202, 0.019, 0.333)	S_{u_4} = 0.477
User 6	30	10	15	5	T_{csp}^{C6}=(0.303,0.454,0.151,0.090, 0.333)	Resultant + T_{csp}^{C6} (0.448,0.338, 0.196,0.016, 0.333)	S_{u_5} = 0.453

Table 4.3 shows the results for cloud feedback based module for the evaluation individual CSP. We took six essential parameters for cloud based feedback module. The registered cloud submitted their feedback through a questionnaire provided by the enrolment module. This questionnaire consist total of six parametric questions about the targeted CSP. The second column reflects the standard score defined by the module. Third, fourth and fifth columns of table represent cloud provider peers submitted feedbacks accordingly. The score of individual attribute is calculated according to the formula shown in table. The final cloud feedback based trust score S_{CLOUD} is calculated in the last column as shown.

Table 4.3: Cloud based feedback based Trust module results

Standard Attributes	**Score Assigned**	**Score by Peer 1**	**Score by Peer 2**	**Score by Peer 3**	**Score of individual Attribute**	**Final Trust score**
					$\mathbf{T}_f = \sum_{i}^{T_{peer}} \frac{(W_i * peer_i}{peer_i}$	
Scalability	0.6	0.4	0.2	0.6	0.6	$\mathbf{S}_{CLOUD} = \left[\frac{\sum_{i=0}^{F_T} \mathbf{T}_f}{\lvert T_{peer}\rvert}\right] * (m * \tau)$ = 0.565
Availability of Data Center Zones	0.6	0.4	0.4	0.4	0.6	
Data Retention	0.4	0.2	0.4	0.2	0.4	
Premium support	0.4	0.6	0.4	0.6	0.4	
Features Stability (Security ,Computing , performance)	0.2	0.2	0.2	0.2	0.2	
Rating (reviews, opinion)	0.2	0.6	0.6	0.4	0.2	

Final trust score $\boldsymbol{T_{SCORE}}$ is calculated by adding the resultant trust scores from the three mechanism used as shown in the table 4.4.

Table 4.4: Final Trust score evaluation and results

Trust scores of individual mechanism	
$\boldsymbol{S_{SLA}} = \frac{\sum_{i=0}^{n}(L_i * SP_i)+(m*\tau)}{\lvert Np\rvert}$ = = 0.56135	$\boldsymbol{T_{SCORE}} = \frac{\boldsymbol{S_{SLA}} + \boldsymbol{S_u} + \boldsymbol{S_{Cloud}}}{3}$ = 0.561+0.453+0.565/3 = **0.5263**
$\boldsymbol{S_u} = p_{f_i} + m_i * \tau_i$ = 0.453	
$\mathbf{S}_{CLOUD} = \left[\frac{\sum_{i=0}^{F_T} \mathbf{T}_f}{\lvert T_{peer}\rvert}\right] * (\boldsymbol{m} * \boldsymbol{\tau})$ = 0.565	

The range of trust is determined by using the table below. This will help in determination of CSP trustworthiness by evaluating the range and level of trust the CSP gained.

Table 4.5: Range of Trust

Final trust score range	**Range of trust**	**Level of trust**
$\mathbf{0 < T_{SCORE} < 0.2}$	ROT 1	**LOW**
$\mathbf{0.2 < T_{SCORE} < 0.4}$	ROT 2	**MEDIUM**
$\mathbf{0.4 < T_{SCORE} < 0.6}$	ROT 3	
$\mathbf{0.6 < T_{SCORE} < 0.8}$	ROT 4	**HIGH**
$\mathbf{0.8 < T_{SCORE} < 1}$	ROT 5	

4.4 Comparative Analysis

SLA, User feedback and clouds feedback are the key factors that contribute trust of the participating clouds. These trust values can be calculated using equation 3.1 (SLA), equation 3.16 (USER FEEDBACK) and (CLOUD FEEDBACK) equation 3.18. To analyze the performance of proposed FCTMM in term of generation of trusted relationship Table 4.6 compares the proposed and existing Schemes in terms of SLA parameters for varying trust values.

Table 4.6: Comparison of trust values with existing and proposed scheme

S.no	**CSP Name**	T_{SCORE}			
		Existing scheme [17]	**Existing scheme [28]**	**Existing scheme [29]**	**Proposed Scheme**
1	**AMAZON**	0.825	**0.3424**	0.425	0.648852
2	**Google App engine**	0.825	**0.3321**	0.548	0.836352
3	**Rackspace**	0.825	**0.3874**	0.448	0.736352
4	**Windows Azure**	0.825	**0.2702**	0.485	0.648852
5	**IBM**	0.825	**0.3702**	0.425	0.748852

It has been observed that using Existing scheme [17] the expected trust values are constant and the results are not varying for individual CSP. In this scheme the SLA parameters considered for calculating trust are limited. Hence the scheme is not showing desirable results and effecting the trusted environment for participating CSP's. The scheme [29] calculates trust by identifying parameters, assigning desirable values and then final trust calculation. The results shows low trust values (0.2 to 0.4) for each participating CSP. These results indicate all the CSP's cannot be trusted to form cloud federation. When the existing scheme [28] is used to calculate CSP's trust, it only considers self, friends and third party recommendations.

As shown in Figure 4.3 it again shows low trust values between 0.4 to 0.6 which indicates that the scheme is not producing satisfactory results for forming trusted cloud federation. It is clearly depicted that when our proposed FCTTM is implemented to

calculate trust values the results are different for each CSP. It considers more SLA parameters than existing scheme along with user feedback and cloud feedback mechanism. The results are hence varying and produce better results than all the existing schemes.

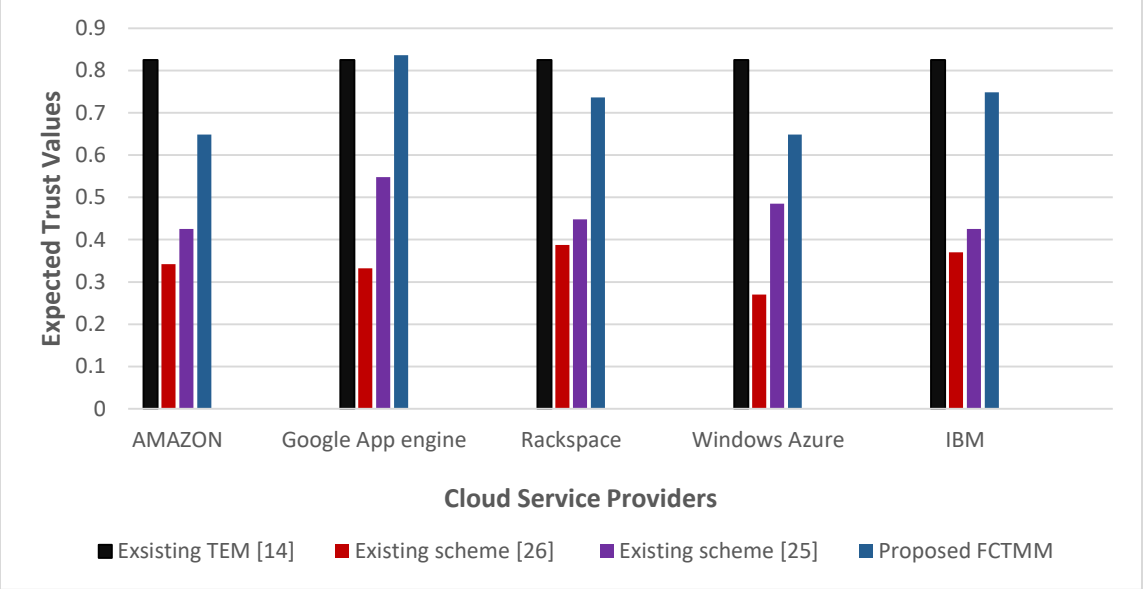

Fig 4.3: SLA based Comparison using existing and proposed schemes between different CSP's

Analysis of Expected Trust Value Based on Number of User Feedback

A significant module of FCTMM is the number of users who are providing feedback related to their experience with the particular CSP. User feedback trust score has the ability to impact the final trust score of participating CSP. In this regard a comparison is done by analyzing an existing scheme [17] with the proposed FCTMM and results are shown in table 4.7.

Table 4.7: Comparison of existing and proposed scheme w.r.t Number of users

S.no	No of users	User feedback S_u		Expected Trust Score T_{SCORE}	
		Existing scheme [17]	Proposed Scheme	Existing scheme [17]	Proposed Scheme
1	6	0.637	0.453	0.584	0.526
2	8	0.66129	0.571	0.595	0.515
3	10	0.5	0.253968	0.542	0.459
4	12	0.435484	0.015873	0.520	0.406

The expected trust values of the proposed and existing trust calculation schemes are analyzed. It includes the overall trust values provided by the users about the participating CSP's. It is evident from the figure 4.4 that the proposed FCTMM method is more reliable and produced better results as the graph is showing a stable pattern. The graph clearly shows that when number of participating user's feedback increases the trust values become stable for a particular CSP. It is because each user faces different experience and as more number of user provides feedback more accurate results are shaped.

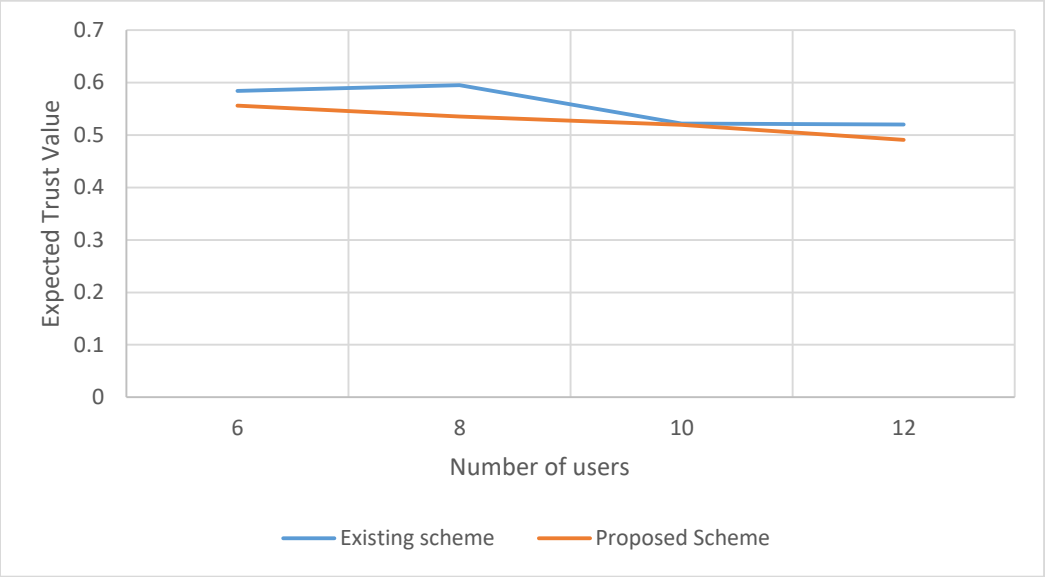

Fig 4.4: Number of User Feedback based Comparison using existing and proposed scheme.

4.5 Conclusion

In this chapter we have discussed and analyzed the proposed FCTMM and concluded that it is practically feasible to implement the proposed model. Moreover the FCTMM is fully complies with the available existing techniques and overcomes the shortcomings of federated cloud trust models. An effort has been done to comprehensively cover conceptual proposed framework over existing techniques and their corresponding implementation methodology.

Chapter 5

CONCLUSION AND FUTURE WORK

This chapter is conclusion to the presented thesis and aims to point towards the potential future research directions. It describes goals of the research carried out and identifies research problems that are still need to be solved by researchers.

Cloud computing as we know is an emerging technology for large scale organizations. It provides advantages to organizations like reducing the cost of IT services by shared computing resources and more data storage space capacity as well as an on-demand and pay per use service mechanism. On the other side many challenges are also associated with CC that includes, trust establishment, data protection from unauthorized access , data recovery and backup availability when in need and data management capabilities etc. Developing customers trust is considered to be most essential of all. In this regard cloud federation is formed by different CSP's to share their resources and satisfy their customers' demands.

In cloud environment to make sure that the customer data is fully secured and standard privacy laws are applied carefully, it is essential to form a trusted relationship and estimate the level of trust between the participating CSPs who want to make a reliable federation. So this research carried out identified the issue of establishment of trusted environment and evaluation of trust level between CSPs as an important requirement and a necessity to take participation in cloud federation for the best utilization of computing resources and customer satisfaction. The research includes comprehensive analyses of existing techniques for evaluation of trust between CSPs in federated environment. A FCTMM is purposed for CSP to ensure the security of critical and sensitive data of their customers and participate in reliable federated environment. Implementation of the proposed FCTMM is done using proposed mathematical equations and obtaining better results.

The purposed model includes three different mechanisms for calculating trust that includes essential SLA parameters, feedback from customers and feedback from CSP's.

The results shows improved trust calculation technique than other existing techniques that will prove to be helpful for both CSP's and their customers. The future directions may include trust calculation based on the following directions.

a) An in depth architectural analysis of CSP for trust calculation which may include study of CSP's hypervisors in trust calculation.
b) Analysis of existing protocols and use of several protocols for trust validation.
c) Recommendation and reputational based analysis of individual CSP's.
d) As with time the level of trust of a cloud provider can increase or decrease In this regard our proposed methodology can further be enhanced to dynamically calculate the trust score based on the risk issues associated with costumer's data in a federated environment.

Appendix A

Set of questions for Customer feedback based trust evaluation.

INSTRUCTIONS: For the following questions please mark ✓ in the ☐ for your feedback.

S #	Questions	Yes	No	NA
1.	Is the connection between you and the vendor's network is adequate?	☐	☐	☐
2.	Do the Service Level Agreement (SLA) of the CSP assure adequate system availability?	☐	☐	☐
3.	Do the scheduled outages affect the system availability you desire?	☐	☐	☐
4.	Would you receive adequate compensation for a breach of the SLA or contract by the CSP?	☐	☐	☐
5.	Do data prevent, corruption or loss occur in redundancy mechanisms and offsite backups?	☐	☐	☐
6.	In case you accidentally delete a file or other data, can you quickly restore it?	☐	☐	☐
7.	Are you allowed to increase the use of the CSP's computing resources?	☐	☐	☐
8.	Can you easily move data to another CSP if required?	☐	☐	☐
9.	Do the CSP use encryption techniques protects sensitive data?	☐	☐	☐
10.	Do the CSP have ability to adjust changes according to your requirements?	☐	☐	☐
11.	Do the CSP have ability to make modifications to its services to keep its service in good repair?	☐	☐	☐
12.	Do the CSP recovery time is adequate?	☐	☐	☐
13.	Do the CSP have ability to operate properly in case of failure of one or more component?	☐	☐	☐
14.	Is the CSP service wise stable?	☐	☐	☐
15.	Is the CSP perform maintenance and correcting problem with ease?	☐	☐	☐
16.	Is the CSP ensures that only personal granted privileges make use of data appropriately?	☐	☐	☐
17.	Can you select the location of data centers to store data?	☐	☐	☐
18.	Do the CSP ensure proper client restrictions on use of data?	☐	☐	☐
19.	In case of data protection breach, do the client get notified?	☐	☐	☐
20.	Are the policies and procedures provide protection unauthorized access or damage?	☐	☐	☐
21.	Is the CSP data retention and disposition processes meet your needs?	☐	☐	☐
22.	Do the CSP provide policies for early contract termination?	☐	☐	☐
23.	Do the CSP adhere to standard processes and policies it commit to follow?	☐	☐	☐
24.	Do the CSP maintains current standard certifications and adopt industry best practices?	☐	☐	☐
25.	Do the CSP provide access to reputable third-party audit reports?	☐	☐	☐
26.	Do the CSP provide a secure gateway environment?	☐	☐	☐
27.	Are the features provided by CSP meet your needs?	☐	☐	☐
28.	Do CSP provide ease in interoperability?	☐	☐	☐
29.	Do the CSP service modification impact usability?	☐	☐	☐
30.	Do the service provided by the CSP need modification?	☐	☐	☐

Appendix B

Set of questions for Cloud service providers feedback based trust evaluation.

INSTRUCTIONS: For the following questions please mark ✓ in the ☐ for providing your feedback.

S no	Attribute	Level of Concern		
		High	Moderate	Low
1	Scalability level	☐	☐	☐
2	Availability of Data Center Zones	☐	☐	☐
3	Data Retention	☐	☐	☐
4	Premium support	☐	☐	☐
5	Features Stability (Security , Computing , performance)	☐	☐	☐
6	Rating (reviews, opinion)	☐	☐	☐
7	Length of time taking services	☐	☐	☐

BIBLOGRAPHY

[1] CloudTweaks, \A history of cloud computing," http://cloudtweaks.com/2011/02/a-history-of-cloud-computing/, 2011, accessed: 2013-01-1.
[2] Personal data in the cloud: A global survey of consumer attitudes. (2017). [eBook] JAPAN: FUJITSU wnloads/SOL/fai/reports/fujitsu_personal-data-in-the-cloud.pdf [Accessed 11 Nov. 2017].
[3] P. Mell and T. Grance, "The nist definition of cloud computing(draft)," NIST special publication, vol. 800, no. 145, p. 7, 2011.
[4] H. Brian, T. Brunschwiler, H. Dill, H. Christ, B. Falsafi, M. Fischer,S. G. Grivas, C. Giovanoli, R. E. Gisi, R. Gutmann et al., "Cloud computing," Communications of the ACM,vol. 51, no. 7, pp. 9{11,2008.
[5] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 1. IEEE, 2012, pp.647-651
[6] M. Stephen, "Formalising trust as a computational concept," Ph. dissertation. University of Stirling, scotland, 1994.
[7] D. L. Hoffman, T. P. Novak, and M. Peralta, "Building consumer trust online," Communications of the ACM, vol. 42, no. 4, pp. 80-85, 1999
[8] Y. Gil and V. Ratnakar, "Trusting information sources one citizen at a time," in The Semantic WebISWC 2002. Springer, 2002, pp. 162-176.
[9] D. W. Manchala, "E-commerce trust metrics and models," Internet Computing, IEEE, vol. 4, no. 2, pp. 36-44, 2000.
[10] L. Zhou and Z. J. Haas, "Securing ad hoc networks," Network, IEEE, vol. 13, no. 6, pp. 24-30, 1999.
[11] K. Aberer and Z. Despotovic, "Managing trust in a peer-2-peer information system," in Proceedings of the tenth international conference on Information and knowledge management. ACM, 2001, pp. 310-317.
[12] A. Tajeddine, A. Kayssi, A. Chehab, and H. Artail, "A comprehensive reputation-based trust model for distributed systems," in Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on. IEEE, 2005, pp. 116-125
[13] R. Chen, X. Zhao, L. Tang, J. Hu, and Z. Chen, "Cuboidtrust: a global reputation-based trust model in peer-to-peer networks," in Autonomic and Trusted Computing. Springer, 2007, pp. 203-215.
[14] U. S. Premarathne, I. Khalil, Z. Tari, and A. Zomaya, "Cloud-Based Utility Service Framework for Trust Negotiations Using Federated Identity Management" IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 5, NO. 2, APRIL-JUNE 2017.
[15] B. Suzic and A. Reiter, "Towards Secure Collaboration in Federated Cloud Environments" 11th International Conference on Availability, Reliability and Security, 2016.
[16] S. Jafari and L. Khatibzadeh , "A Multi-Factor Trust Management System Based On Confidence In M-Commerce Environment" , Second International Congress on Technology, Communication and Knowledge (ICTCK 2015) November, 11-12, 2015.

[17] A. Kanwal, R. Masood and M. A. Shibli "Evaluation and Establishment of Trust in Cloud Federation" International Conference on Ubiquitous Information Management and communication (IMCOM, 14') Columbia January 9-11, 2014.Mohammed Alhamad, Tharam Dillon and Elizabeth Chang "SLA-Based Trust Model for Cloud Computing" 13th International Conference on Network-Based Information Systems, 2010.
[18] F. Rajibabaei and M. R. Y. Moghaddam , "Proposing a centralized trust management system to detect compromised node in WSN" , 3rd International Conference on Computer and Knowledge Engineering (ICCKE 2013), October 31 & November 1, 2013.
[19] S.Chakraborty and K. Roy, "An SLA-based Framework for EstimatingTrustworthiness of a Cloud"IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.
[20] D. Wallom, M. Turilli, G. Taylor and N. Hargreaves, "myTrustedCloud: Trusted Cloud Infrastructure for Security-critical Computation and Data Managment", hird IEEE International Conference on Coud Computing Technology and Science, 2011.
[21] S. M. Habib, S. Ries and M. Muhlhauser, "Towards a Trust Management System for Cloud Computing", International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11-FCST-11,2011.
[22] S.M.Habib, S.Ries, S. and Muhlhauser, M. (2010). Cloud Computing Landscape and Research Challenges Regarding Trust and Reputation. 2010 7th International Conference on Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing, pp.3-6.
[23] M., T. Dillon, and E. Chang, (2010). SLA-Based Trust Model for Cloud Computing. 2010 13th International Conference on Network-Based Information Systems, pp.1-4.
[24] A. Jøsang and D. McAnally, "Multiplication and comultiplication of beliefs," International Journal of Approximate Reasoning, vol. 38, no. 1,
pp. 19{51, 2005.
[25] P. Patel, A. Ranabahu, and A. Sheth, "Service level agreement in cloudcomputing," 2009.
[26] SLA in Cloud Computing Architectures: A Comprehensive Study. (2017). International Journal of Grid Distribution Computing, 8(5), pp.7-32.
[27] J. Hughes and E. Maler. Security assertion markup language (saml) v2. 0 technical overview. OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-08, 2005
[28] S. Singh and D. Chand, Trust Evaluation in Cloud based on Friends and Third Party's Recommendations. (2014). Chandigarh: RAECS UIET.
[29] S. K. Garg, S. Versteeg and R. Buyya, "SMICloud: A Framework for Comparing and Ranking Cloud Services", 4th IEEE International Conf. on Utility and Cloud Computing, Dec. 2011, pp. 210 – 218
[30] T. Velte, A. Velte, and R. Elsenpeter, Cloud computing, a practical approach. McGraw-Hill, Inc., 2009.
[31] D. L. Hoffman, T. P. Novak, and M. Peralta, "Building consumer trust online," Communications of the ACM, vol. 42, no. 4, pp. 80-85, 1999
[32] S. Jones, M. Wilikens, P. Morris, and M. Masera, "Trust requirements in e-business,"
Communications of the ACM, vol. 43, no. 12, pp. 81-87, 2000.

[33] A. Jøsang and D. McAnally, \Multiplication and comultiplication of beliefs," International Journal of Approximate Reasoning, vol. 38, no. 1, pp. 19-51, 2005.

[34] P. Patel, A. Ranabahu, and A. Sheth, \Service level agreement in cloud computing," 2009

[35] A. T. Akinola and M. O. Adigun, "Feedback-based service selection in ad-hoc mobile cloud computing," 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), Durban, 2016, pp. 172-177

[36] V. V. Rajendran and S. Swamynathan, "Parameters for comparing cloud service providers: A comprehensive analysis," 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, 2016, pp. 1-5.

[37] K. Visram, "Review: Eclipse for Java Developers," in ITNOW, vol. 46, no. 4, pp. 30-30, July 2004.

[38] J. Hughes and E. Maler, “Security assertion markup language (saml) v2. 0 technical overview," OASIS SSTC Working Draft sstc-saml-techoverview-2.0-draft-08, 2005.

[39] B. Kaplan and D. Duchon, “Combining qualitative and quantitative methods in information systems research: a case study," MIS quarterly, pp. 571-586, 1988.