International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-10 Issue-4, February 2021

A Secret data sharing Model for Agriculture Experts in Federated Cloud based on Polynomial based Encrypted Scheme

V. Keerthi, T. Anuradha

Abstract: ***A shift in computation from PC's to Cloud allows more number of users to involve in cooperative computation on various categories of data wish to merge their expertise and thereby gain more useful information without leaking their own sensitive information. In the case of data collected from various sensors in an agricultural farm IoT device, the cloud and customers can cooperate to provide adequate services; benefits to experts, research stations related to agriculture. Enormous Agriculture Data generated is related to Soil, weather, Research, crop, farmers, Agriculture marketing, Agri-IOT, fertilizers and pesticide makes cloud as a centralized resource.The exchange of information and research will inculcate a healthy competitive atmosphere in the country in agriculture. Sharing of data, computation, services across cloud boundaries with different clients at different places will enhance expertise suggestions and results to farming field which benefit to improve countries economy. Federation of cloud will allow resource and data sharing, but the security threats severely limit the application development as the usage of data processing or sharing mechanisms will leak private information. So in this research paper, a Polynomial Based Encryption Secret Sharing Scheme (PBESSS)is proposed as Federated cloud data exchange system with multiple cloud instances of the same cloud host or separate computing hosts.***

Keywords: Cloud, Federated Cloud, Different data types want to combine their capabilities and thus gain more useful information without revealing their own sensitive data. In the event of data gathered by various sensors in the IoT system from farming fields in agriculture, the cloud and customers can co-operate to provide suitable services, Security, Data sharing scheme, Agriculture experts , Polynomial based encryption, Secret sharing.

I. INTRODUCTION

People's lifestyles have changed dramatically due to Speedy Internet of Things growth, mobile computing, big data and cloud computing . The cloud computing plays an important role in providing a dynamic, secure and customizable ecosystem that ensures service quality to customers at anywhere ubiquitously. Cloud computing, is a service oriented technology that has revolutionized the Business of information and communication technology (ICT). The cloud delivers all as a service (XaaS) ,which can be accessed at anytime from anywhere on a pay-per-use model.Ssavings Inspire corporations and enterprises to implement cloud technology for their software demands during initial capital investments and operating costs[1]. Cloud Computing technology increases collaboration, mobility, elasticity and availability and creates cost savings opportunities by streamlined and efficient computing. Cloud computing has been defined by the U.S. Global Standards and Technology Institute (NIST) as: "A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". This cloud model encourages availability and consists of five core features, three distribution models and four implementation models [2], [3], . Though the cloud computing offers many benefits as IT resources can help respond to evolving needs of an enterprise at low cost, its adoption is slow as the CSP (Cloud Service Provider) cannot ensure the data confidentiality, integrity, authentication, and availability. In Cloud computing Security problems are the most important obstacles which have to be addressed for client adoption and satisfaction. Believing theCloud can have the capacities for maintaining protected data collection, tight access management, reliable and efficient consumer data backup, such as a trustworthy encryption system. As the cloud helps users to achieve processing capacity that goes outside their own physical realm and generate different security threats, such as access management, authentication and detection, availability, convergence of policy, auditing . Along with above , cloud computing faces some of privacy issues which include Protecting personal records, transaction history and confidential data, avoiding improper secondary use, loss of user access management, undefined data privacy obligation, etc. Cloud Computing is meant to shift the computing load to the shared networks. This proposal would trigger the issue of customer's private information being exposed to the possibility of unwanted access and retrieval that needs to be handled properly[4]. Since cloud can be used by more number of users which allow them to involve in cooperative computation, The owners of different data forms, without revealing their own sensitive data, would like to combine their tools to gain more usable information. In case of scientific experiments, which require expertise computation in weather, health, agriculture fields by sharing data, requires protection of their private data.

Manuscript received on February 08, 2021.
Revised Manuscript received on February 15, 2021.
Manuscript published on February 28, 2021.
* Correspondence Author
V. Keerthi*, Ph.D Scholar, Department of Computer Science, School of Science and Technology, Dravidian University, Kuppam, Chittoor, Andhra Pradesh, India. Email: keerthiuha@gmail.com
Prof.T.Anuradha, Dean, Department of Computer Science, School of Science and Technology, Dravidian University, Kuppam, Chittoor, Andhra Pradesh, India.. Email: rajamaata@yahoo.co.in

Similarly Data obtained from various IoT device sensors can be aggregated to deliver the targeted result; the cloud and its users can collaborate to provide the necessary services. Security risks seriously hinder the use and popularisation of this technology because sensitive information is always leaked . Hence, The development of multi-party data processing methods that safeguard privacy has become an essential research task to be addressed in short time. To overcome resource shortage Inter-Cloud or federation computing has been introduced. Federated cloud model provides access to resources from various services, through a well defined SLA (service level agreement) between service provider and customer . This can be applied to various fields not only to business ,scientific but also to agriculture domain in which this paper is proposed. In this paper section II gives federation cloud and security issue, Section III gives some of the related works , Section IV gives brief discussion about data Sharing between Agri-Experts in Cloud, section-V discusses Federated Cloud Data usage by Agri-Experts and sections VI,VIII and VIII have given proposed PBESSS scheme for secure data sharing along with protocols and working module, and further implementation details.

II. FEDERATED CLOUD AND SECURITY

Today, as the complexity of task increases more and more computation power is required, so as the computers and working environments are becoming more and more distributed. It is not possible to have infinite resources in cloud to provide it to client. If request exceedsIt cannot provide customer support with sufficient computing and storage capacity. The Inter-Cloud discusses situations where each cloud uses the device, storage and other cloud computing services. A type of Inter-Cloud, known as Federation Cloud allows set of cloud providers to interconnect to share resources among others. Governmental clouds or Experimental clouds in fields like Health, Weather, Agriculture etc., will require this type of arrangement to provide huge computation, storage or any other sharable resource[5][6]. Security concerns which spans cloud computing will also applies to Federation computing. The effects of cyber-attacks on federated cloud will have significant economic consequences. The more concerns will be in case of loss of some data, individually, as the federation may span across different networks. In Cloud federation, for the cloud service providers, achieving security is complex due to heterogeneity and dynamic nature of systems running various client applications. Cloud federation with complex computations and dynamically changing configurations will have different security requirements [7]. Some of the problems include the shared infrastructure and virtualization technology, complexing in identifying attacks due to lack of collaboration among cloud service providers, No distributed databases are used among Cloud federation clients to detection attacks and to implement defense strategy, different policies are used in cloud federation by system security administrators.

As we know that applications of new technology like Mobile Computing, Cloud computing, IOT, Big data analytics and processing help in leaps and bounds to improvise our traditional Agriculture system. These new tools, methodologies and best practises are used by agricultural researchers and experts to share data to bring modern techniques to increase production. Different advances in the field of IT display some promising signals for productive and smart agriculture. With the emergence of software-defined cloud environments that promote large-scale and real-time analysis of data, the rapid adoption of artificial intelligence (AI) advances, tools for the visualisation of knowledge, the growing range of smartphone applications are to transform farmers' lives in the days ahead. The exchange of information and studies will instil a healthy competitive atmosphere in farming throughout the world . Sharing of data, computation, services across cloud boundaries with different clients at different places will enhance expertise suggestions and results to farming field which benefit to improve countries economy. So in this paper, a secure data sharing model between clients and agriculture experts at different cloud service providers acting as federated cloud is proposed to share data to carry on computations related to agriculture experiments

III. RELATED WORK

Even though Cloud infrastructure enables organisations to host their own computing services securely, flexibly, and cost effectively, hackers, attackers and security scientists have research and evidence that this paradigm can be abused and not fully protected . So security throughout cloud model should be improved for its better adoption. Data sharing, exchanging etc., operations are common in most of applications of cloud. As it is also a part of cryptography, which is known as Secret sharing refers to any process by which a secret is spread among a group of individuals, each allocating a share of the secret. The secret is only opened after certain conditions are met. There are a number of participants each, and a group of t (threshold) or more shares can open up confidentiality together, but no group less than t can retrieve shares anonymously. Research work by [8] given about secret sharing schemes which can be solved by number theory and bitwise XOR, Chinese Remainder theorem, as well as by using polynomial interpolation by shamir and by Blackley's which is based on hyper plane geometry. But it is difficult to implement. In Paper[9], Chunming Tang ,Zeng-an-yao, have discussed secret sharing scheme which Consists of two simple protocols: I a distribution protocol where secret K is spread between the participants by the dealer, and (ii) a restoration protocol with respect to the secret K is recovered. Basic schemes such as threshold secret sharing and verifiable secret sharing to solve the problem that all players in the scheme are honest and also to avoid all participants' dishonesty, are proposed respectively.

Shi Runhual et.al [10] has suggested a multi-secret sharing regime where more than one secret needs to be revealed, which is the normal expansion of the secret sharing scheme where multiple secrets are to be exchanged, and each secret will recreate this secret with numerous professional subsets of participants. Jakson et al. divided multi-secret programmes into two groups in 1994: one-time and multi-use [11]. When those secrets are reconstructed in a one-time-use system, the secret holder needs to redistribute fresh shares to each member. On the other side, each party in a multi-use system must hold just one share. The distribution of shares to each member can be a very punctual and expensive process. A common downside shared by nearly all established secret sharing programmes is that they are one-time processes. Secret sharing schemes are important in cloud computing environments in terms of group of stake holders sharing secret data. Especially in cloud federation when a secret is to be shared between tenants in same cloud or in different cloud this type of secret sharing mechanism is used. So a secret sharing scheme, which can be used in agriculture field when a secret is to be shared between agriculture experts using applications running in same cloud or in different cloud providers is proposed in this paper Daniel Augot and Matthieu Finiasz[12] have proposed a public key cipher scheme related to the Polynomial Reconstruction(PR) problem. In this scheme, at one side Alice's The public key is generated as a kind of noise, which correlate with the Polynomial Interpolation problem and is based on the hidden data of Alice. Then, as Bob tries to relay a message to Alice, he randomises this noise, adds it to the message and adds a random little noise from himself. Then Alice will use the hidden knowledge as a trapdoor to eliminate Bob's additional noise. This thesis is based on two new assumptions of intractability: while PR is used to evaluate the public key's stability, encryption protection depends on the obvious complexity of decoding a Reed-Solomon inserted by one letter. Although various issues exist in Federated cloud environment as a part of this paper a concern of security to be addressed in this environment is studied. In case of attack it should be detected and steps to be taken to avoid failure in services and given idea of IDS for security[13] . Authors Tobias Wuchner et.al, in their paper[14] have discussed cloud storage federation issues for single-provider problems such as service maintenance and protection of the data storage at different providers, rather than storing data at only one location. How the data is to be distributed and replicated at different cloud storage providers for reduction of vendor lock-in and high data availability is also discussed. At the end they have addressed the solution for transparent data distribution and replication on the provider-side in federation but not during data sharing.

In paper [15] when data is distributed across cloud or in Federation of cloud there is increasing need for integrating and querying data across distributed and autonomous data sources. It leads to a challenge to ensure privacy, interoperability, and scalability for such data services. Although data or services are dispersed within a federation, the method masks them on the horizon and emerges as a single virtual data source or consumer data service, which is then available as if part of a single structure. Mainly two concerns such as data federation services' privacy and protection restrictions should be tackled such as data security by service providers (e.g. institutions) who would like to protect their data or data possession. The issue of privacy security for data in the federal setting is complicated since the data is spread between CSP's. In multi-party estimates, current privacy structures in single provider settings and protection notions do not properly resolve the risks in the distributed environment. Yan-e Dan[16] addressed the features of farm data and how the knowledge management system of agriculture is useful in the field of agriculture. Yifan Bo, Haiyan Wang[17] analysed and proposed that in agriculture and forestry, the new IOT and cloud computing technology can be used in accurate agriculture management. In his paper he pointed out problems in defence, IPV6, management of data centres, etc. The paper [18] had given a description of an application of cloud for agriculture, and cloud-based monitoring platform to monitor agricultural resources by using Aduino and Sensors that are relevant for data transmission to the self-implemented Heroku cloud platform. The variables used were soil moisture (volume water percentage), humidity, atmospheric temperature, dew point and soil temperature and are studied and further action will be automatically taken by the system. Paper[19] has stated that even though field of Agriculture plays major part in economy of India, farmers They are isolated, unorganisationed, illiterate, capital poor and are at high risk of natural hazards, financial instability and price crashes. Through this, an information library with a rich conventional and scientific knowledge of agricultural fields will be built into a cloud-based ERP (Enterprise Resource Planning) and an e-agriculture network for resource planning to empower agricultural confraternity. The availability of an automated e-agricultural ERP-Cloud facility for accessing all sorts of information would help farmers with personalised solutions across geographical areas. and experts in various regions share information to update data or to create a new technology.

IV. DATA SHARING BETWEEN AGRI-EXPERTS IN CLOUD

In this online computation age, cloud computing technology is very helpful for storing enormous Agriculture data related to Soil, weather, Research, crop, farmers, Agriculture marketing, Agri-IOT, fertilizers and pesticide as a centralized resource in the cloud as shown in figure-1 below. In case of research, agriculture experts residing at various locations of globe can share data and scientific achievements at cheaper cost to all the developing nations to cope up agriculture production. Now-a-days every aspect is connected to automation, agriculture farms works are automated with help of IOT, Drone technology etc., which requires big processing support at background like cloud computing technology.

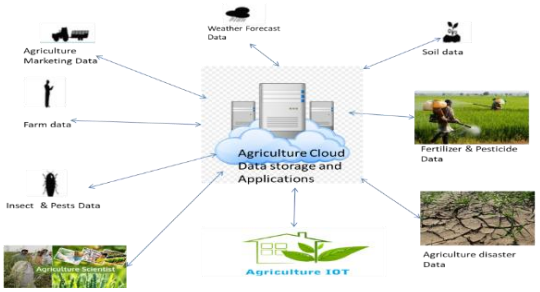

Figure 1 Agriculture Domain applications to Cloud

V. PROPOSED FEDERATED CLOUD DATA SHARING FOR AGRI-EXPERTS

In this paper Polynomial Based Encryption Secret Sharing Scheme (PBESSS) is proposed as a Federated Enterprise data sharing system for different cloud instances (each instance relates to Agriculture expert or any client to share agricultural data) belonging to the same cloud host or separate computer hosts. In case of research, agriculture experts residing at various locations of globe can share data and scientific achievements at cheaper cost to all the developing nations to cope up agriculture production. At the same time, security issues related to data sharing may cause loss or change of data by malicious users at cloud. In order to overcome this, a new data sharing scheme has been proposed. Assuming each agricultural expert residing in cloud instance or at different cloud want to share data secretly without compromise for computation, the following scheme is designed. Each Agri-expert at cloud instance will share his/her data secretly without knowing other hosts data thus ensuring privacy and achieve the final result. Cloud host providers share data between multiple cloud environments to solve the n^2 link. Whenever Agri-expert requests support from a cloud host provider and whether this is a complicated programme request the calculation is based on the resource resources of other cloud host. If possible a group of cloud-based agri-experts as seen in Figure-2.

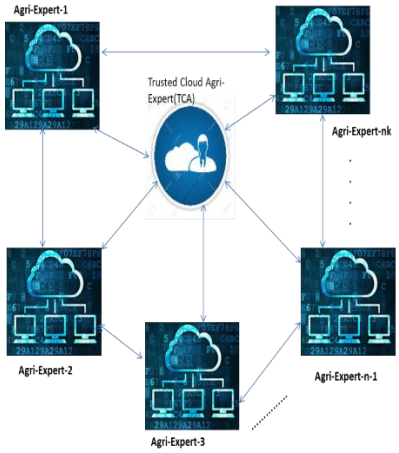

Figure 2 Federation of Clouds used by Agri-Experts for data Sharing

Among these cloud instances or experts residing at Cloud one becomes Trustworthy Cloud Agri-Expert (TCA), who manages and directs the full computing. TCA will request and accept passwords, or it will use them to initialise a secure data sharing system with hidden keys if it already has credentials for any agri-expert in the cloud-instance. TCA can create a session for a specific instance of computation on request from the client/application and session IDs are dynamically generated for each host engaging in computations. Session IDs are submitted privately to all cloud hosts in the federation. Session-id can be used for authentication when each of them exchange data during computation. Internally, cloud hosts would provide coordinators to manage the SLA computation. The method suggested uses SMC[12], but the secret value used in the knowledge exchange process is encrypted, which is hard to realise since a DL strategy is being used and each cloud will eventually decode the final value using its secret keys. The hidden value of this scheme is therefore not exposed to TCA since it is encrypted by hosts using their own keys.

VI. ALGORITHM POLYNOMIAL BASED ENCRYPTION SECRET SHARING SCHEME (PBESSS) FOR FEDERATED CLOUD ENVIRONMENT

After Initialization of clouds in Federated environment with Trusted Cloud Agent(TCA) with necessary parameters, sharing of data mechanism process workflow will be initiated by TCA and operation will follows as shown below.

1. Exchange of Credentials between TCA and Agri-Experts from Cloud locations in Federated Cloud .
2. Private key generation g_i for Clouds in Federation for secure secret Exchange.
3. Generation of Secret polynomial based on Primitive number by each Cloud in Federation.
4. SMC implementation between Clouds in Federation to compute Sum of polynomials to retrieve Secret.

The steps are depicted in sequence Diagram shown in Figure 3.

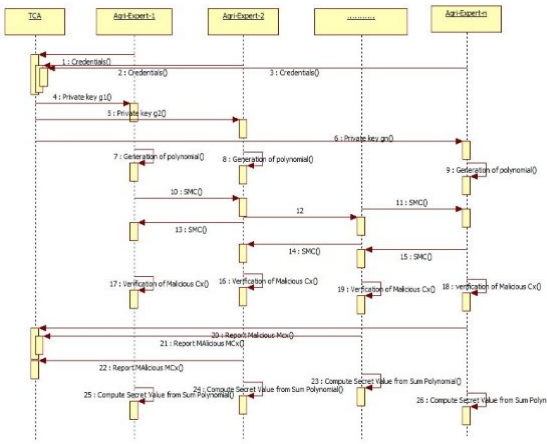

Figure: 3 sequence diagram of proposed Polynomial Based Encryption Secret Sharing Scheme (PBESSS) for Federated Cloud Environment

5. Public keys k_i, t_i for individual Secret value verification and δ function for secret value recovery.
6. Verification of Malicious cloud using Malicious_Cloud_Verify() by C_i among the federation.
7. If Malicious_Cloud_Find(MC_i) = True, Reporting MC_{ix} to TCA to avoid in final value computation.
8. Recovering Secret from Sum(Final) polynomial for each Cloud(C_i) in federation.

VII. WORKING OF PROPOSED POLYNOMIAL BASED ENCRYPTION SECRET SHARING SCHEME (PBESSS) FOR FEDERATED CLOUD

The suggested scheme is used to protect confidential data when exchanged between federated clouds during computation. In this scheme the secret data is encrypted and decrypted by the each cloud to retrieve original value while SMC is used between them to exchange of data. It is assumed that Following expectations, TCA and cloud hosts are safe to share data at the configuration point, and all cloud services are truthful without a malicious nature. The scheme **PBESSS** between multi-parties is used between Agri-Experts in Federated cloud for secure data sharing. This scheme is more secure since each party generate itss own polynomial based on generator g_i which is secret to each agri-expert participating in computation in which secret value in it is encrypted and will be verified at the verification phase. Each polynomial is constructed using coefficients from Galois field (GF) consisting of primitive elements with the group ZN_{pi}* created from generator g_i.

The **PBESSS** data sharing scheme works in following phases as

1. Initialization Phase: Initializes Trusted Cloud Agent/Admin(TCA) and Agri-Experts participating in Computation scheme.
2. Distribution Phase : each agri-expert in federated cloud (participants of secret sharing) Exchange machine secrets to obtain the final polynomial Encrypted hidden meaning.
3. Verification Phase : In this phase, each agri-expert in federated cloud Checks the hidden value by decrypting and finds the malicious host Trusted Cloud Agent/Admin or rejects its value.
4. Recovery Phase: In this phase each agri-expert after verification phase, recovers the secret by using necessary protocols by each Agri-expert in federated cloud.

VIII. PROTOCOLS PROPOSED BETWEEN TCA AND AGRI-EXPERTS IN POLYNOMIAL BASED ENCRYPTION SECRET SHARING SCHEME (PBESSS)

In specifyig the proposed data sharing scheme for agri-experts in cloud, some assumptions are made and are to be strictly followed at the time of executing the scheme. The assumptions are specified below.

1. All the agri-experts, service providers of clouds in federated cloud and Trusted Cloud Admin/Agent (TCA) are supposed to be honest in the Initialization phase while sharing the credentials so as to make TCA to generate secret keys.
2. The network is secured and keys are not hampered during Distribution Phase.
3. All agri-experts and TCA follow a secure technique in verification Phase.
4. Recovery phase is done as per the protocols given by TCA thus avoiding, non-repudiation.

The following protocols are defined for proposed PBESSS:

a. Initialization Protocol between TCA and Agri-Experts at Federation cloud ($Acex_i$)

b. Distribution Protocol between TCA and Agri-Experts at Federation cloud ($Acex_i$)

c.Verification & Reporting Protocol between TCA and Agri-Experts at Federation cloud ($Acex_i$)

d. Recovery Protocol between Agri-Experts in Federation cloud ($Acex_i$)

The following notations are used in protocols

Notation	Description
TCA	Trusted Cloud Agent/Admin
DC_i	Digital Certificate for i^{th} Agri_Expert at Federated cloud
$Acex_i$	i^{th} Agri_Expert at Federated Cloud
FC	Federated Cloud
GF	Galois Field over Znp_i
MD	Message Digest

Table 1: Notations used in PBESSS model

a) Initialization Phase Protocol between TCA and $Acex_i$

In this phase TCA(Trusted Cloud Agent) will start session and session id's are sent secretly to all agri-experts in Federated cloud that participate in computation. Then TCA by using (DC_i) digital certificate of i_{th} expert in Cloud, computes and sends private and public keys to all experts participating in computation. TCA is selected by agri-Experts in Federated Cloud, which will monitor the data Sharing Scheme or TCA is announced to all Agri-Experts participating in Data Sharing scheme for computation for combined experimental result.

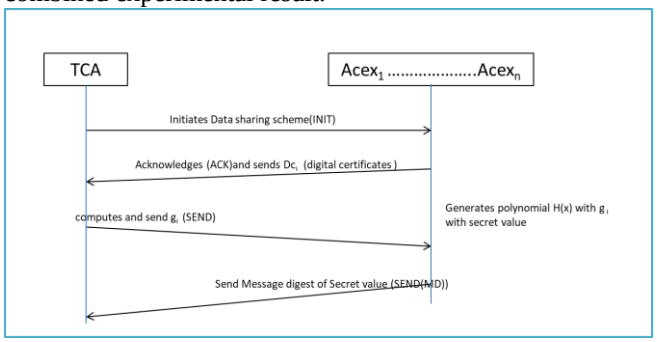

Figure: 4. Initialization Protocol between TCA and Agri-Experts

b). **Distribution Protocol for Agri-Experts at Federation cloud ($Acex_i$)**

In this phase, all the agriculture experts in Federated cloud participating in Computation of exchange secrets to achieve final polynomial with secret value in encrypted form uses Distribution protocol.

1. Each $Acex_i$ in Scheme call Create_Polynomial() process to construct polynomial secretly with each Coefficient a_i in primitive polynomial $H_i(x)$ is the primitive number in $GF(g_i^{bi})$ where $0<i\leq n-1$ and a_0 is secret value of each party $Acex_i$.
2. Each $Acex_i$ call Compute_Secret($H_i(x)$,n) which computes, $a_0= s_i d_i$ where $d_i=(g_i^{bi})\delta_i$ where $\delta_i \in Z_{Npi}^*$ such that $g_i^{bi}\delta_i \equiv 1 \bmod N_{pi}$, here s_i is the secret that is to be shared between experts during computation.
3. Each agri-Expert in Federated Cloud party, $Acex_i$ calls PBESMC($H_i(x)$,n) to implement Multi-party Computation (SMC) scheme and computes final sum polynomial $H(x)= \sum_{i=1}^{n} hi(x)$ and coefficients are in GF, and sends it to TCA for verification.

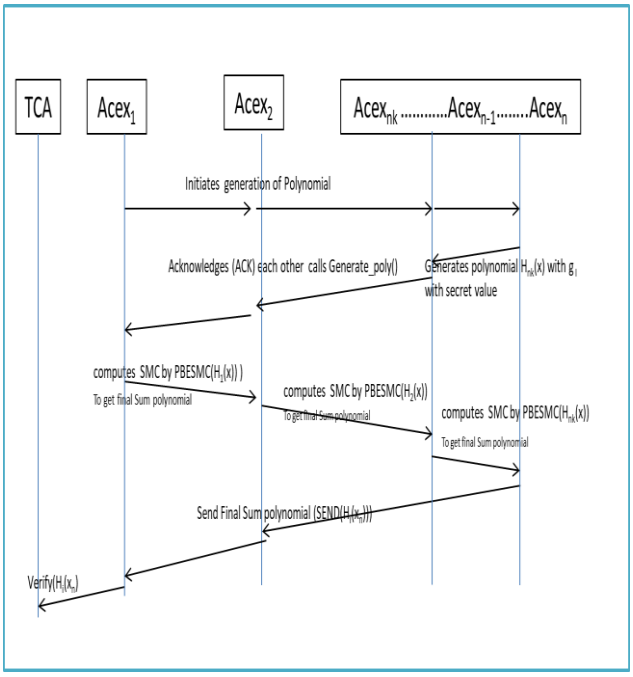

Figure: 5 Distribution Protocol between Agri-Experts for Final Sum polynomial computation

c. Verification & Reporting Protocol between Trusted Cloud Authority (TCA) and Agri-Experts at Federation cloud ($Acex_i$)

In this phase each Agri-Expert in federation cloud uses Verification & Reporting Protocol and verifies the secret value by decrypting which finds the malicious host, if exists, and reports to Trusted cloud Authority(TCA) or rejects its value.

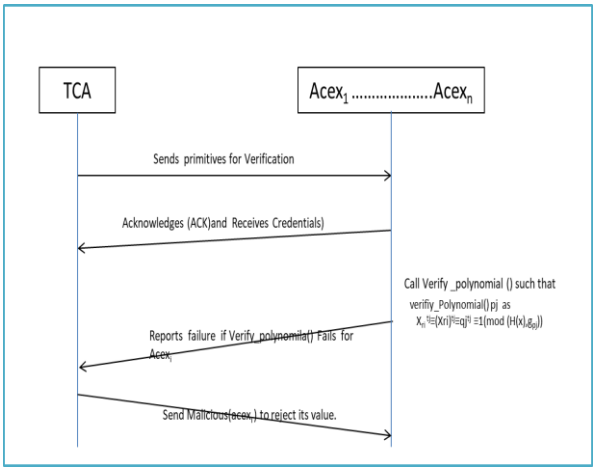

Figure: 6 Verification and Reporting Protocol

d. Recovery Protocol for Cloud experts $Acex_i$ for secret value in computation

In the recovery phase Agriculture experts at cloud $Acex_i$, after verification and reporting malicious expert $Acex_k$, the secret is recovered by using following steps of protocol by each expert in federated cloud. In this protocol it is assumed that Secret can be recovered even if there exists m ($m<n/2$), is a fallacious agriculture expert in cloud.

1. Each $Acex_i$ finds secret $s=\Sigma(s_i d_i)$ where $d_i=(g^{bi})\delta_i$ where $\delta_i \in Z_{npi}^*$ such that $g_i^{bi} \delta_i \equiv 1 \bmod n_{pi}$
2. $Acex_i$ calls Recover_SValue($H_i(x)$,n) to find Sum of all polynomials to recover secret value 's'
3. TCA sendSecretMD(s_i,n) to $Acex_i$ each expert verify secret value S whether it is correct or modified or any fault in computation, so that integrity is maintained.

Further recovery phase of PBESSS can be applied to the three cases as in SMC in recovering secret, it malicious cloud host exists during data sharing or data recovery then it is distributed among experts in Federated cloud.

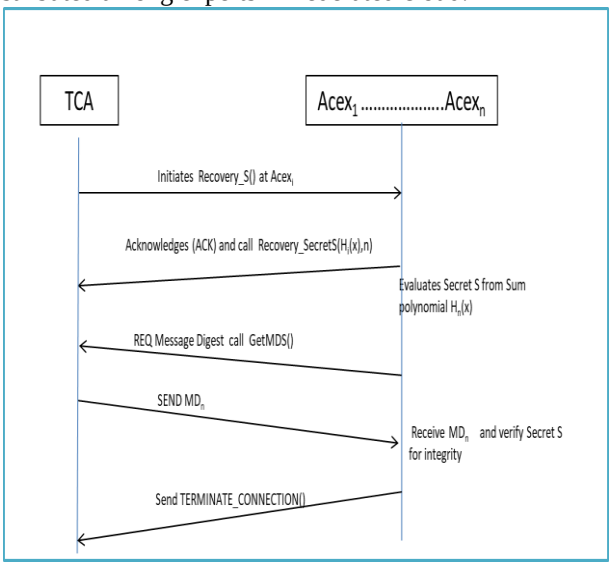

Figure: 7 Recovery Protocol for Secret 's' by $Acex_i$

IX. EXPERIMENTAL IMPLEMENTATION OF PBESSS

The proposed PBESSS scheme can be implemented in Federated Cloud environment and the communication between TCA and Agri_Experts will take place in secure manner. The modules in Scheme can be designed as Libraries and interfaces for user through SaaS service, can be implemented in Java or in Python. Simulated cloud environment can be created by using OpenNebula, Eucalyptus [20] ,Aneka cloud platform which provides open source solutions. API's in OpenNebula provides inter-cloud capabilities and usage. The federated environment which is represented below in Figure 8, shows that TCA and Agri_experts will be located at different clouds at various locations with different IP addresses . Experts who want to participate in complex scientific algorithm/ technique computation to get secret value , will be under control of TCA and operate through Federated Cloud control Management Console. TCA will control and co-ordinate activities between Agriculture($Acex_i$) during the implementation of PBESSS scheme.

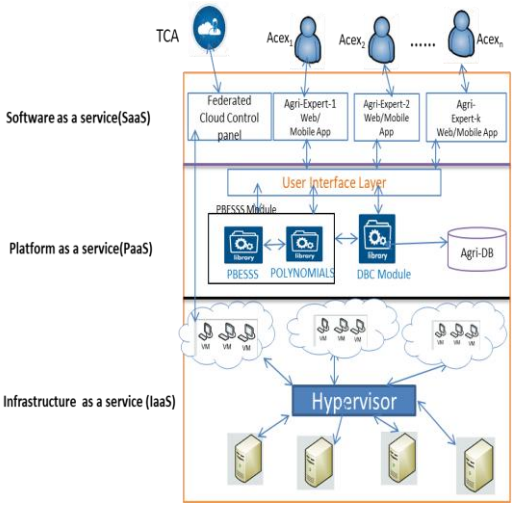

Figure: 8 High level Diagram of TCA and Agriculture Experts in Federated Cloud

As computing demand increases for consumers a large computing resources across multiple regions is essential, to address their application needs. Single cloud provider may not be able to address such requests due to lack of resource or its presence or capacity in multiple regions. For this concern the solution is addressed by using Federation of cloud or Inter-Cloud. Using this technical approach multiple cloud entities can work in alliance to form a bigger cloud entity with massive resource capacities. Open source tools can be considered which can simulate our federated cloud application to run. For this propose OpenStack can be used for its implementation and can be simulated/ or modeled. At PaaS the proposed model can be divided into modules PBESSS module which comprises Poly-Module to be called by application at higher level SaaS layer, which acts as an interface to Users.

X. CONCLUSION

The cloud computing and federated cloud with some of the security issues is stated. Application of Federated cloud to Agriculture field and its usage by experts in agricultural field is studied. In this paper secure multi-party data sharing scheme in cloud, a PBESSS scheme between TCA and agri-experts along with protocols at various phases are given. The model of implementation of PBESS scheme is given in simulated Federated Cloud Environment. The various clients/agri-experts involved in process of data sharing and computation using the cloud resources running at SaaS layer can use PBESSS service at PaaS layer in cloud through internet. The results and implementation will be given in future publications.

REFERENCES

1. Samee U. Khan, Elements of cloud adoption, may 2014, IEEE Cloud Computing
2. NIST SP SOO-145 , "The NIST Definition of Cloud Computing", http://csrc.nist. Gov/publications/drafts/SOO-145IDraft-SP-SOO-145-clouddefinition .pdf, NIST Special Publication SOO-145, January 2011
3. Rajkumar Buyya, John Wiley & Sons, Inc., Publication, 2011. Andrzej Gocinski "Principles and Paradigms of Cloud Computing."
4. Actually. Wang, "Security and Privacy Issues within the Cloud Computing," 2011.
5. World Computer Sciences and Information Technology Conference, Chengdu,
6. Chinese, 2011, p. 175-178.
7. N. Grozev and R. Buyya. Inter-Cloud architectures and application brokering: Taxonomy and survey. Software Practice and Experience, Softw. Pract. Exper. 2014; 44:369–390
8. C.H. Hsu et al. (Eds.): ICA3PP 2010, Part I, LNCS 6081, pp. 13–31, 2010.© Springer-Verlag Berlin Heidelberg 2010.
9. MacDermott, Áine & Shi, Qi & Merabti, Madjid & Kifayat, Kashif. (2014). Security as a Service for a Cloud Federation., The 15th Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet2014),June 2014,Research Gate.
10. Binu V P, Sreekumar A, Simple and Efficient Secret Sharing Schemes for Sharing Data and Image, International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 404-409
11. Chunming Tang, Zeng-an-yao, N.S., 2008 International Threshold Secret Exchange System.
12. Advanced Computing Theory and Engineering Conference,IEEE,2008
13. Shi Runhual, Huang Luo Yonglong, Zhong Hong, A Multi-Secret Threshold Sharing
14. Scheme, 2008 IEEE Networking, Sensing and Control International Conference
15. W.-A.Jackson, K.M. Martin, C.M. O'keefe, Asiencrypt, 1994, pp. 42-54, "On sharing many secrets,"
16. Daniel Augot and Matthieu Finias, A Polynomial Public Key Encryption Scheme
17. EUROCRYPT 2003, LNCS 2656, pp. 229–240, 2003 Restoration Problemz
18. The 15th Post Graduation Symposium on Integration of Telecommunications and Networking and Broadcasting (PGNet2014) in Liverpool, Study Gate [13] Defense as a cloud service
19. IEEE International Cloud Conference, IEEE, Tobias Wuchner, Steffen M¨uller and Robin Fischer,2013.
20. Pawel Jurczyk, Li Xiong, Slawomir Gorieszka, DObjects:Enabling Data Federation Systems Privacy-Preservation, 2012 IEEE 28th International Data Engineering Conference, IEEEE
21. Yan-e Duan, "Design of Intelligent Agriculture Management Information System Based on
22. *IOT",* IEEE, Fourth International Smart Computing Technology and Automation Conference 2011
23. Yifan Bo, Haiyan Wang, "*The Application of Cloud Computing and The Internet of Things in Agriculture and Forestry ",* International Joint Conference on Service Sciences, IEEE computer Society,2011
24. Kayode E. [18]. Adetunji; Meera K. Joseph, Cloud-based monitoring system creation

25. 4Duino: Applications in Agriculture, International Big Data Developments Conference 2018, Systems for Computation and Data Sharing (icABCD), IEEE
26. Tameem Ahmad; Shamim Ahmad et.al, Indian agriculture related knowledge: with cloud agreement ERP, 2015 Green and Internet of Things (ICGCIoT) International Conference, IEEE
27. Sowmya.P,Kumar.R, Federal Cloud Deployment Strategy, Asian pharmaceutical and clinical science journal, April 2017, ISN 2455-3891.

AUTHORS PROFILE

Mrs .V. Keerthi pursed Master of Computer Science from Sri Venkateswara University, Tirupathi and Master of Philosophy in Computer Science from Dravidian University, Kuppam in 2017. She is currently pursuing Ph.D. in Dravidian University, Kuppam. Her main research work focuses on Cryptography, Information Security in Cloud She is having 4 years of teaching experience.

Mailid:keerthiuha@gmail.com

Prof. T. Anuradha is working as a professor in the department of Computer Science and Dean, School of Science and Technology Dravidian University, Kuppam. She did her Ph.D. from Sri Padmavathi Mahila University in Tirupathi. She has 23 years of teaching experience. Her research areas are Data Mining & data warehousing, Neural Networks, Cloud Computing, Wireless Sensor Networks. She has published good number of journals in the same areas.