Secured and Provisioned Access Authentication using Subscribed User Identity in Federated Clouds

Sudan Jha[1], Sultan Ahmad[2]*, Meshal Alharbi[3], Bader Alouffi[4] and Shoney Sebastian[5]
School of Sciences, Christ (Deemed to be University), NCR, New Delhi, India[1]
Department of Computer Science, College of Computer Engineering and Sciences
Prince Sattam Bin Abdulaziz University, Alkharj, 11942, Saudi Arabia[2, 3]
Department of Computer Science, College of Computers and Information Technology
Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia[4]
Department of Computer Science, Christ (Deemed to be University), Bangalore-29, India[5]

Abstract—**Cloud computing has become an essential source for modern trade or market environments by abled frameworks. The exponential growth of cloud computing services in the last few years has resulted in extensive use, especially in storing and sharing the data on various cloud servers. The current trend in the cloud shows that the cloud owners use relative functions and target areas in such a way that cloud customers access or store their data either in the same servers or related servers. Simultaneously, from the security point of view, the lack of confidence about the customer's data on the cloud server is still questionable. The hour's need is to provide the cloud service in a 'single port way' by forming the joint management policy to increase customer satisfaction and profitability. In addition to this, the authentication steps also need to be improvised. This paper discusses issues on the security authentication and access provisioning of the cloud service consumers in federated clouds using subscribed user identity. This work proposes the user identity verification module (UidVM) in the cloud service consumer's authentication process to serve as a cloud broker to minimize the work overloads on the central cloud federation management system, thus enhancing the cloud security.**

Keywords—Security authentication (SA); cloud federation (CF); cloud service provider (CSP); key distribution center (KDC); user identity verification module (UIdVM)

I. Introduction

Cloud computing is a rapidly growing technology to share/store data on the cloud server in a cost-effective manner (Timely and financial effectiveness). Cloud computing is a distributed-based service to the remote data consumer. Nowadays, cloud computing is used as a significant source and framework for modern trade or market environments. Consumers adapted to the online cloud service buy and sell products, and many of them spend their time accessing and share cloud resources daily. This has also led cloud computing technology to business society. Therefore, any number of people who are business owners prefer cloud services. Cloud computing technology helps enterprises and organizations make computing their resources addressable to the partner and consumer to achieve a more scalable, flexible, competent, and cost-effective circle for application development [1]. Presently, cloud-computing domains (public, private and hybrid clouds) furnish different services to minimize the repairing costs on various cloud services.

As described in [2], the initially formed cloud computing model has reached a high level of evolution, exposure to various extents to settle the primary characteristic of the prototype resource argument, interpose of services, lack of interoperability in data representation, quality of service degradation, and others.

A. Cloud Computing Service Providers (CCSP)

Cloud computing is the panoramic concept in the recent computing technology explained in several ways by many researchers. However, cloud computing is an unspecific term for the transaction of the distributed services in the networked hosts. It provides easy accessibility for the companies to use computing resources (e.g., an application, virtual machine) as a utility rather than developing by their own. In short, cloud computing is accessing/storing programs and data/resources over connected networks as an alternative using an individual hard drive/storage device.

The purpose of 'Cloud Computing Service Providers' (CCSP) is to solve cloud computing problems. These joint CCSPs are formally called cloud federations and are responsible for handling the most critical situations [3]. Cloud federation has been one of the murmuring terms since long when the issue of transacting from users' resources to the remote cloud server was raised. The issue was the transaction through an easy and pervasive way of accessing [4]. Different models have been discussed in this regard; however, cloud computing was built with the dual combinations of the cloud computing deployment model and cloud computing service model.

B. Cloud Computing Service Models

Cloud computing service model is a combination of three services/models. Software as a Service (SaaS to help in using the cloud applications on consumer devices running on the cloud infrastructure as provided by the respective cloud providers. [5]. Platform as a service (PaaS: which provides platforms to allow the service consumers to develop, run, and control over all the cloud applications by removing the complicated building and maintaining of the cloud infrastructure [6] and thirdly, Infrastructure as a service (IaaS which is the fundamental resources access provider on the cloud infrastructure. Physical and virtual machines, load balance, virtual storage, etc., are the essential resources availed

*Corresponding Author.

to the end-user through virtualization of the server. IaaS is used to deploy network platforms to provide the consumers with the process, storage, and other basic activities and computing resources. IaaS provides virtually limitless scalability, reduces infrastructure costs, and accelerates time to market [7,8].

C. Deployment Level of Cloud

This model means the mechanism or the ways of lay-outing the cloud structure that seems like on the actual environment. There are three basic types to deploy cloud computing. These are public cloud layout, private cloud layout, and hybrid cloud layout, but the NIST clarified into four as defined in [9]. There is a community cloud in addition to those three listed.

Private cloud: It provides strongly secured services used exclusively by the institution that owns the infrastructure and maintains full control over it. The private cloud infrastructure is planning for alone use by a standalone institution comprising multiple consumers (e.g., business units). It is governed and administrated by single private institutions/units.

Community cloud: is refers to an IT infrastructure owned and shared for collaboration between the group of institutions having common concerns. A community cloud is essential and more beneficial for the community cloud environment. This infrastructure is prepared for alone use by limited ownership of consumers from an institution with mutual concerns.

Fig. 1 and Fig. 2 demonstrate how the public cloud, hybrid cloud, and private cloud interact with the community with their respective service models. Fig. 1 is focused on SaaS, PaaS, and IaaS in terms of their application, platform, and infrastructure.

Public cloud: This cloud is open and accessible for all consumers. The type of clouds will provide the best economies of scale for the users, are inexpensive to set-up because It is open for the broad number of users on the internet. The public cloud is managed, operated, and governed by business, academic, governmental institutions, or by their joint.

Hybrid cloud: it is reasonable and more manageable for the cloud consumer and service provider, making the unity by collectively from two or more than two well-defined cloud infrastructures such as private cloud and community cloud [10].

The union of private and public clouds forms hybrid cloud. A cloud federation is a collective and collaborated cloud organization within agreed interests and common characters of consumers with (1) geographical dispersion, (2) a briefly and clearly defined commercialization system, and (3) federate agreement that governs a collection of independent and heterogeneous clouds. It should be confident enough to furnish impressive resource scalability, guarantee service performance, realize the dynamic distribution of participating resources, and respect end-to-end Service Level Agreement (SLA) established with its clients, as shown in Fig. 2 [11].

Objectives Motivations: The paper's main objective is to perform user authentication in the federated cloud providers using the subscribed user identity to access cloud service consumers' provisioning and maximize their satisfaction while using any cloud services.

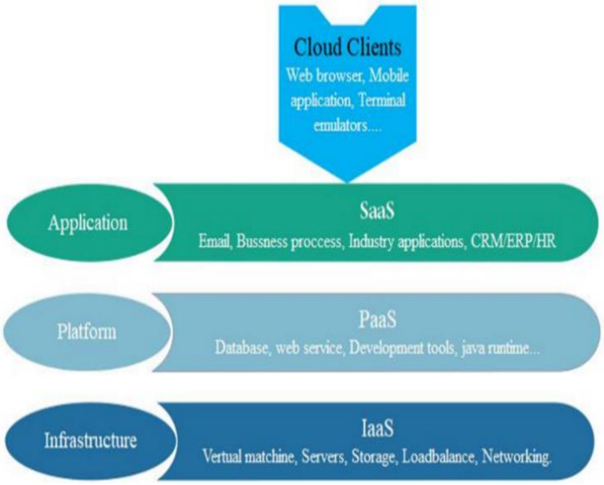
Cloud Clients
Web browser, Mobile application, Terminal emulators....
Application
SaaS
Email, Bussness process, Industry applications, CRM/ERP/HR
Platform
PaaS
Database, web service, Development tools, java runtime...
Infrastructure
IaaS
Vertual matchine, Servers, Storage, Loadbalance, Networking.

Fig. 1. Cloud Computing Service Models Arranged as Layers in a Stack.

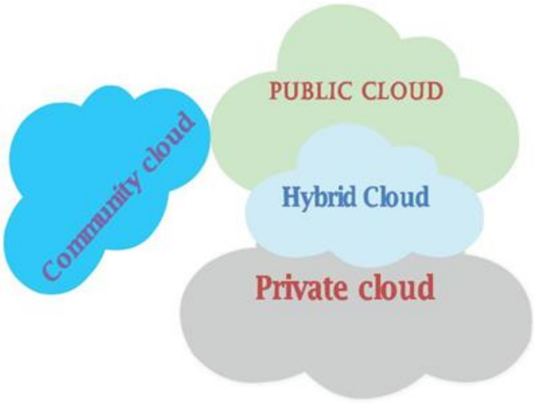

Fig. 2. Cloud Computing Deployment Model.

Many proposals regarding cloud federation are focus on architecture and benefits. There is a good number of works performed by many researchers regarding architecture and structural flows. Several kinds of research have been carried out on security authentication for cloud computing services.

However, in this paper, we aim to point out some sets of limitations. Sorting out these limitations will enhance the security authentication of cloud federation, since cloud federation is a collection of (a) volunteers and (b) 'agreed cloud servers/cloud service providers' who have some common goals to share the services in a central administrator or cloud management. i.e., there are many communications between the cloud federation members and the cloud consumer on the remote side. In this work, we aim to interact with the cloud service providers to resolve this kind of security vulnerabilities, including security authentication.

In this paper, we have calculated the convergence time with respect to a particular range of federation size and showed that the results obtained from our proposed model clearly indicate the effective reduction of the time consumption when the CSCs are using multiple identities to access the resources on multiple CSPs. Our proposed model also gives a dual combination of the cloud computing deployment model and the cloud computing service model.

Our contributions in this work are as follows:

1) Its calculated the convergence time wrt a particular range of federation size and show that the proposed model effectively reduces time consumption when using CSCs multiple identities to access various CSPs resources.

2) The proposed model gives a dual combination of cloud computing deployment and cloud computing service model.

3) Our results prove that time consumption is adequate while accessing the resources.

4) Our work proposes a CSP's consumers access provisioning model (algorithm) by which work-overload is reduced on the central management system. i.e. 25 logIn executions are executed in 3115 milliseconds (Fig. 10).

The rest of the paper is organized in the following order. Section 2 gives a background study about related work. Section 3 consists definitions of basic components that are involved in the cloud federation management system. In Section 4 the contribution of our proposed work is discussed. Section 5 has result and discussions. Finally, Section 6 concludes the paper and future scope.

II. Background Study

Many works related to cloud computing security and cloud federation identity management and security authentication have been published. The related papers that are relevant to our paper are discussed as follows selectively. Several researchers examine and determine the characteristics of cloud federation to formalize it. The author of [3] describes the cloud federation as an intentional pooling of heterogeneous clouds running cooperatively to share idle resources contained in their domains and presents the cloud federation properties. These [1] allows the cloud server in the federation to automatically spread out resources to satisfy themselves, have high promotional opportunities of their resources to the remote cloud service consumers in the environment and to be highly competent in the modern market system, permit the clouds to offer idle resources and stakeholders to use the resources, and deliver services with defined requirements in service level agreement (SLAs).

A. Authentication and Authorization

A user centric approach, [12] provides a solution for the cryptographic process. In [13], paper discussed about the approval as well as responsibility of trust model. FermiCloud [14] followed the different protocol for the model but it took longer process of certification. In [15] given the idea, how to manage the cloud complexity with the help of software application. The different access control facilities are followed in the [16] model.

B. Unique Key Access

In [17] discussed about how to identify the unique cloud properties and manage those properties for the use of third parties. Stihler et al. [18] token methodology for the secure level of services. In the paper [19] given the two different authentication of encrypt the data and digital sign of the process. The paper [20], cloud storage system support for public users with the identity proof. The [21,22] proposed different architecture for managing the cloud. In [23] followed the x and y access implementation virtual softwares.

C. Confidentiality, Integrity, and Availability

Santos et al. [24] extend the Terra [25] followed the different level of implementation in the virtual storage of infrastructure and different level of services. They discussed about the various methodology and procedure for accessing the stored information. Popa. et.al to access the group of data from the cloud. In [26], they also followed the fuzzy techniques for utilize the cloud resources. The author explained about the threats in cloud server, how to manage with open source application [27]. In [28], followed the supervisor techniques for remote controlling the procedures. The synchronize response of cloud and protocols are followed in the virtual cloud [29].

D. Security Policy Management

In [30] studies the cloud federation security issues about managing and controlling the access of an authorized party. It proposes a federated access control model (FACM) in which a third party, like a cloud service broker (CSB), is used. On the other hand, authors in [31] and [13] describe the federated cloud's benefits over the single cloud service briefly. They described from the user and cloud service provider's perspective and listed benefits for the cloud federation, which are highly scalable and flexible to enable the cloud providers to cost-effectively or cost-efficiently adjust their hosting capacity through cooperation with other single clouds. It shows the federated clouds relation and authentication. Still, it does not show how the remote cloud service cloud consumers can be authenticated to access the federated clouds on their proposed cross-cloud federation.

On the other hand, in cloud federation, the cloud consumers can retrieve services from different service providers without requiring multiple authentication processes using SSO techniques [32], [14].

Amazon cloud service provides a wonderful and robust secured service in the world [33][34]. Still, it does not make federated clouds in the market system with the other cloud service providers which are in working on related discipline (online shopping). According to [1], [9], [14], [17], cloud federation has various mutual benefits for the cloud service providers to use other service providers' infrastructures and/platforms based on their agreement. It is beneficial for both service providers and service users to efficiently and cost-effectively provide and consume cloud resources [35][36]. The federated clouds should authenticate themselves in the cross-cloud federation because cloud security is the responsibility of cloud service consumers and cloud service providers [4]. In the federated clouds, the cloud service consumers (CSC) should access the federated clouds using subscribed user Identity.

Conclusion of the background study/related works: The studies done in this section conclude that though most of the work published explores the possibility of the new features, they only discussed the benefits/advantages of cloud service providers in the federated clouds. The works that are analysed in the literature clearly mention that cloud service customers and cloud consumers are categorized into two segments, and cloud customers can get access provision in the federated clouds. However, the cloud consumers possess denied access using the single cloud accounts in the federated clouds.

III. Prerequisites / Definitions

Components: The following are the basic components that are involved in the cloud federation management system. Here Cloud Federation Central Management System/Key Distribution Center (CFCMS/KDC) depicts the central management of the federated cloud and governs all over the transaction between cloud service providers (CSPs). It has all information about the federated clouds that agree to implement their communications in the cloud federation. We have used KDC instead of CFCMS as the alternative name, but not an abbreviation form. We have also used KDC instead of CFCMS in the designed algorithm.

UidVM: is the User identity Verification Module installed between cloud service consumers and cloud service providers because it acts as a mediator between the CSP and CSC. It registers the (cloud service consumers passcode) CSCpc MainDataCen-terId to make the connection between CSCs and CSPs. It creates healthy, safe, and fast communication between the CSCs and CSPs.

CSP: It is the cloud service provider federated in the cloud and governed under the cloud federation rule and provides the service to cloud service consumers.

CSC: is the cloud service consumer that accesses the provided data from the service providers.

CSCpc: The cloud service consumer's passcode is generated from the central system and verified by UidVM to get cross access permission.

The activities of cloud providers can be divided into various categories: Implementation support, utilize the resource, maintain the support, and protection.

The protection feature necessary for cloud providers' activities are described in Table I [11].

TABLE I. Security and Privacy Factors of the Cloud Providers

Security Context	Description
Approval and Verification	These process of cloud identification schemes are followed.
Management of Authenticity and Availability	Heterogeneous techniques are followed in the service.
Secrecy, authenticity, and accessibility	Trying to assure the secrecy of data objects, enabling factors accounted, and making sure that assets are available if needed.
Observing and Issue Resolution	The cloud infrastructure is constantly monitored to ensure adherence with consumption data protection and auditor's report.
Strategy Administration	Creating and making regulations for concrete behaviors such as monitoring or conformity evidence.
Privacy	To protect the identification information for the cloud.

Prerequisites: Currently, cloud computing has been leading almost all business, education, and social communications. Many public and private organizations and institutions are connected through the internet, sharing and storing their data in the cloud. The cloud users may use one of these public, private, hybrid, and community clouds or others that they may create depending on their organization's infrastructure. In short, various sectors (e.g., educational, health, communications, military, etc.) are now become cloud service dependent.

The fundamental issue of cloud computing is that its security management system and ownership issues are complained about by the cloud service consumer. For solving these issues, the cloud is classified into the public cloud, private cloud, and hybrid cloud. On the other hand, community clouds have a long history with the emerging of cloud computing.

Recently inter-cloud, cloud federation, and other cloud infrastructure models have emerged. Whatever it is, our focus is cloud federation, which is one of the recent cloud models. Cloud federation is the best solution to reduce the infrastructure building cost, the increase business relationship between the cloud providers, the availability and accessibility of the cloud providers, etc.

Current Troubles of cloud federation: Even-though, cloud federation has several benefits and advantages for a cloud service provider, there are challenges and troubles raised by the cloud service consumers and cloud providers. As our survey and observation, we have listed below.

Security issue: Accessing and sharing of the data is still a questionable issue.

Load balancing: The cloud federation architecture can be designed in such a way that the central cloud federation server does more workload on the central cloud federation management system. More workload also leads to high traffic, and the server becomes slow to send or respond to the cloud service provider. Therefore, minimizing the central system workload is one of the critical issues for fast service.

LogIn steps: Today, users prefer fast-track accessing methods. Users of Cloud service consumers want the short and secure step to access online services (Cloud services). But, currently, the provisional service procedure has very boring and continuous steps to permit the service consumer to access the cloud resources. Therefore, this paper aims to shorten and remove such continuous steps of Cloud service provision (LogIn) for the cloud service consumer to access the cloud services.

Inclusion of the third intermediator: There is a need to include the cloud service consumer for authenticated access to share the services' benefits by minimizing multiple processes of login and accessing the data using the subscribed login accounts in the federated clouds.

IV. Proposed Model

Our proposed model has used the data to depict the cloud federation's various characteristics on both sides (cloud service provider and cloud service consumer). The simulations are carried out in CloudSim. Referring to recently published works [12], [14], we see that it is very difficult to perform actual/real-time experiments and implement new algorithms and technologies in actual cloud infrastructure. Therefore, we measured performance implementation first.

A. *Proposed Model Motivation*

Currently, many organizations and institutions are organized in a single group to form the cloud federation. From the perspective of cloud consumers, the need to use cloud resources is increasing. Still, some business cloud service providers (e.g., online shopping) don't have an agreed federated cloud system to access their customer's permission to use the subscribed account in the federated cloud. The online shopping companies' common goals are available and accessible to the online purchasers, and online purchasers also want to access and buy the product using their subscribed user account in the federated clouds. Therefore, our motivation is to reconcile that the CSP's need and CSC's need by proposing how the CSPs and CSC are authenticating each other using subscribed Identity in the federated clouds to assure the security between CSPs and CSCs.

B. *Proposed Security Authentication*

The cloud federation requires two sets of (improvised) proposed rules, Service Level Agreement (SLA) [23], and Regional Service Condition Agreement (RSCA) [21]. SLA sets on the cloud federation central management system and agreed by the cloud service providers to govern all the interactions and resource sharing conditions between the CSPs. On the other hand, there may be a high load of CSC's service requests, which leads to work overload on the central system. RSCA handles this issue, and it is installed in the cloud federation central management system (CFCMS).

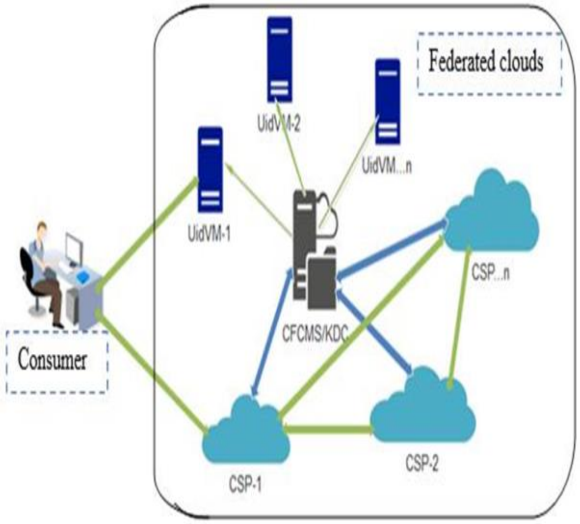

Fig. 3. Proposed Cloud Federations Architecture.

Security Authentication: It is performed between the cloud service consumers and cloud service providers. The cloud service consumers with cloud service providers through KDC and User Identity Verification Module (UidVM), if it is cross-cloud service in the federated clouds, and cloud service providers each other through CFCMS using the Cloud Federation Security Authentication Key Distribution Center. All cloud service consumers and cloud service providers' information related to security authentication is registered on UidVM. All the agreement documents between the service providers and the regional code are placed on the cloud federation central management system (CFCMS) called the Key Distribution Center (KDC) that directs the user verification to different modules connected to the KDC. Fig. 3 shows the proposed cloud federations authentication architecture, and Fig. 4, the general diagram for CF authentication. Both Fig. 3 and Fig. 4 show the general flows that how users and providers' security authentication is performed).

C. *Cloud Service Provider Authentication*

Cloud service provider authentication is performed on cloud service providers to use the shared resources in the cloud federation infrastructure according to their agreement and authentication. They perform through a cloud federation central management system using a key distribution center to verify that the cloud server is registered or not in the federation. As shown in Fig. 4, when the authentication is performed, the following steps apply sequentially.

The cloud service provider sends the request to the cloud federation central management system or KDC. Cloud federation central management system verifies the cloud service provider's membership and other conditions based on the federation agreement.

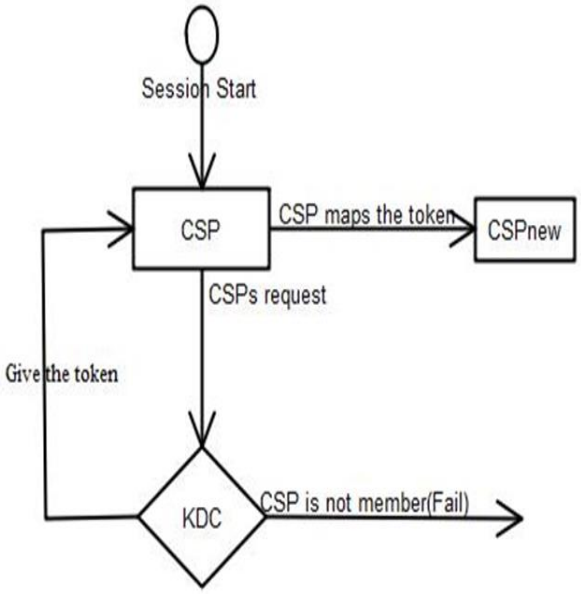

Fig. 4. State Diagram for Cloud Service Providers Authentication.

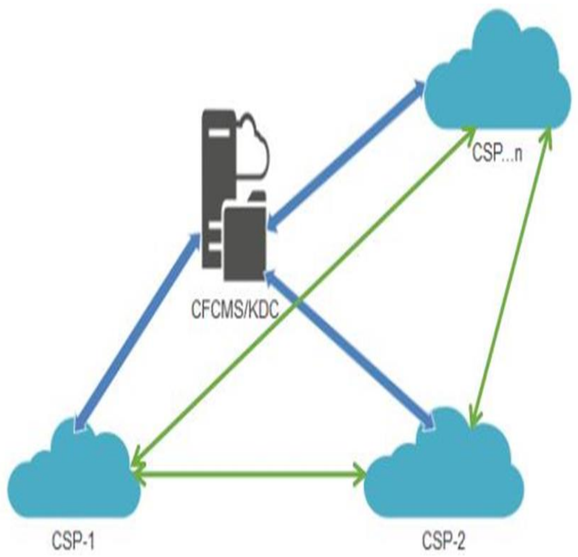

Fig. 5. The Process of Cloud Service Providers Authentication.

A cloud service provider gets permission and starts to access all resources regarding to the federation members' security agreement. As depicted in Fig. 5, cloud service consumer/user authentication is performed through a cloud federation central management system using a key distribution center. It helps the cloud service consumers access the federated clouds with a subscribed identity in any one of the federated clouds. Fig. 6 gives more insight details/highlights. When the authentication is performed, the following steps are applied sequentially.

(Note: Cloud service provider is a single cloud server owner that provides the service to the remote cloud service consumers).

Step 1: Cloud service consumer is a remote cloud service user/consumer that provides by the cloud service provider.

Step 2: Consumer/user sends the service request to the cloud service provider (to one of the federated clouds that the consumer has a registered account).

Step 3: Cloud service provider server verifies the user is registered or has an account.

Step 4: Cloud service provider gives access permission to the user on its own server. But, if the user wants to access other service providers (cross-service), then.

Step 5: User request to KDC to get the cross permission for another service provider's server through the current CSP, which is the user already registered.

Step 6: KDC sent the user's request to the UidVM after verifying the incoming request region.

Step 7: UidVM verifies the user and gives the token to the user to access other service providers in the federation.

Step 8: User maps the token to another cloud service provider server.

Step 9: User gets access to all federated clouds with the Subscribed login account.

D. Algorithm 1: Access Provision for Cloud Service Consumer

The following algorithm initializes every cloud service consumer and checks if these consumers are previously registered in the cloud or not. For registered consumers, access provisioning is checked by analyzing the CSC request. Based on this analysis, the grant of local permission or global permission is availed. Else, the access provisioning is denied. This enhances the convergence time and reduces the time consumption in the particular federation size.

```
Initialize: (CSC=Cloud Service Consumer, CSP=Cloud Service Provider)
do
if (CSC CSP) Check that if csc has registered account in csp or not exist.
if CSC have registered account in CSP then local controller analyses the CSC request, that if it is local access permission request or global(to another csps)
(CSC     CSP) // if request is local, then CSP gives access permission to CSC
while
CSC CSP // here CSC does not exist in CSPs database that is why CSC is now denied the access permission
end
```

E. Algorithm 2: Cross Access Provisions for CSCs

Algorithm 2 maintains the central repository for each member and checks their validity. If membership is valid, then the access is provisioned to the member, thus allowing the member to enter into the cloud (cloud federation). These members are now mapped with the new resources and compare the clouds' utilization, whether they are overloaded or not or crossing the allocated time frame. If any of these occur, the member is allowed to access the cloud federation to reduce the overload.

```
Initialize: (CSC=Cloud service consumer, CSP=cloud service provider, UidVM=User identity Verification module, KDC=key distribution center, CSPn=new cloud service provider,
do
for (CSP 2 KDC) // Central management system check CSPs membership.
UidVM KDC//after checking the csp membership and sign, KDC give the access permission to CSP)
for (CSCpc 9 UidVM) // check the CSCPS in UidVM or not exist
UidVM// if CSCPC is exist in UidVM then UidVM give the token to CSC
CSC // CSC maps to the new CSP for resources.
while
CSP 2= KDC // Cross access provision is continued until CSP is
leave from the federation membership.
CSCPC @ UidVM// Cross access provision is continued through the federated clouds until CSCPC is EXIST in UidVM.
end
```

F. Algorithm 3: Load Balancing

Algorithm 3 calculates the execution time to handle the idle UidVM. A central management system can identify the idle or less loaded UidVM when calculating the on-progress tasks corresponding to the number of UidVM.

1 Initialize: (Initialize: How CFCMS calculate and identify the less loaded UidVM.

Let, number of on progress user request (nopur) =g, number of UidVM=h, UidVM= f, and number of waiting user request (nwur) =e. (g=nopur, h=nUidVM, e=nwur, f=UidVM.

(Please refer the short note above)

```
2    do
3    for (f < g/h)
4    f e // Assign the next waiting task to UidVM.
5    while
6 f > g/h
8 end
```

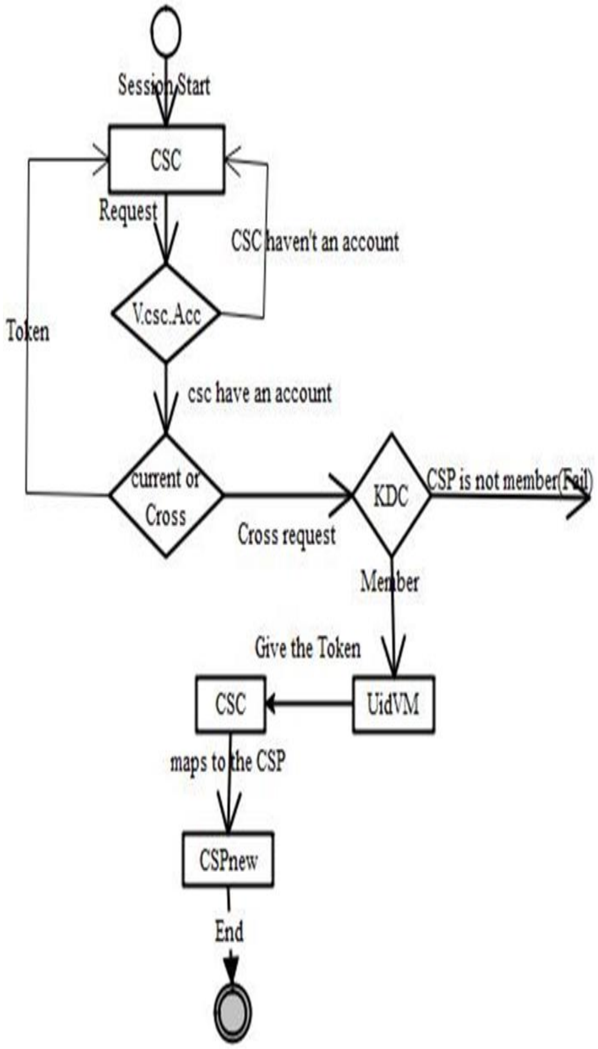

Fig. 6. State Diagram for Cloud Service Consumer/User Authentication.

Table II compares the proposed model with previously proposed models with respect to the three parameters Overload, Insurance, and access provisioning. Table II shows that previously published work is basically focused on ensuring the federated cloud security, assuring CSCs benefits, whereas, in our proposed model, we have illustrated by implementing subscribed identities to access the cloud resources from multiple cloud service providers. And from the results (Fig. 7, Fig. 8, Fig. 9, and Fig. 10), we can observe the effective reduction of the time consumption when the CSCs are using multiple identities to access the resources on multiple CSPs; i.e., our paper not only ensures or assures but validates them.

TABLE II. COMPARISION OF OUR PROPOSED MODEL WITH PREVIOUSLY PROPOSED MODELS

Factors/parameters	Proposed model	Existing scenarios
Overload	- identifies an idle module - calculates the time duration of each task, and then it reduces the idle UidVM. - Therefore, reduction of work overload on the central management system is effective and better ever	- In [32], idp (identity provider) is responsible for identifying all the incoming requests - gives privileges according to their legal information. - As a result, it leads to high work overload on Idp.
Insurance	- Ensuring the security of the federated cloud through KDC and UidVM, including removal of duplicate data	- Ensure security by removing the duplicating data (only) on the cloud server database [12]
Access provisioning	Tries to assure the CSCs benefits in the federated clouds and threats them equally with the CSPs.	- More focus on the benefits of cloud service providers rather than the CSC regarding access provisioning. - It doesn't work with other Cloud service providers [4], (example, online shopping)

V. RESULT AND DISCUSSION

We now compare our work with the most recent works that has been published recently as Table III.

Based on all the algorithms and the results obtained, we observe that.

1) Cloud service consumers can access the cloud resources using their subscribed id without any other requirements for each of CSPs in the federated clouds. This reduces the execution time when multiple users are using in the cloud federation considerably.

2) Work-overload is reduced on the central management system. Fig. 10 shows that 25 login executions are executed in 3115 milliseconds. That means the CFCMS can make communication and verification without any overload in around 3 seconds.

TABLE III. COMPARISON WITH RECENT WORKS

Year	Outcomes	Outcome of our proposed work
2017 [20] S.Ye, H. Liu, Y.-W. Leung, and X. Chu et. al.	- Used ADL to access the Cloud service - No subscribed id used - Reduction in the execution time is very low as they have used a software-defined technique (ADL) and the code complexity is high. - No discussion on multiple users where is it is evident that in today's scenario, a cloud is hit by multiple users in practical it goes up to trillion hits in a minute	- No requirements for each of CSPs in the federated clouds. - Reduced execution time
2017 [21], Katakam Srinivasa Rao et.al.	- Collective motion is a fundamental operation of robot swarms - A group of Reinsurance emulated Collaboration Mechanism in Cloud Federation is defined - Doesn't yield out the execution time - No reduction in the cloud performance evaluated - Cloud federation is discussed in detail, but no subscribed ID has been used to evaluate cloud computing time.	- No requirements for each of CSPs in the federated clouds. - Reduced execution time

We, therefore, conclude that

1) CSP consumers have a high access provision.

2) The execution time is reduced, when multiple users are using cloud federation.

3) Efficient reduction in the work overload with 25 logins that too in 3115 milliseconds, as in Fig. 10.

4) Also, CFCMS communication and verification (without any overload) is in around 3 seconds.

The comparative results are depicted in Fig. 7, Fig. 8, and Fig. 9.

Fig. 7 shows an Efficient Reduction in the work overload with 25 logins that too in 3115 milliseconds. There is an efficient reduction in the execution time when multiple users are using in the cloud federation.

In Fig. 8, the federation size is evaluated from 2. We see that the convergence time is very high at each and every federation size for various work overloads. In this case, also, reduction is efficient and the work overload is attempted at minimal logins with minimal time.

Fig. 9 shows that each cloud service consumer's convergence time has maximal access to the cloud resources at every federation size. For this, we have performed extensive use of the data in cloud storage to save bandwidth and minimize the storage space. Again, there is a reduction in the execution time when multiple users are using in the cloud federation without any need for data deduplication authorization.

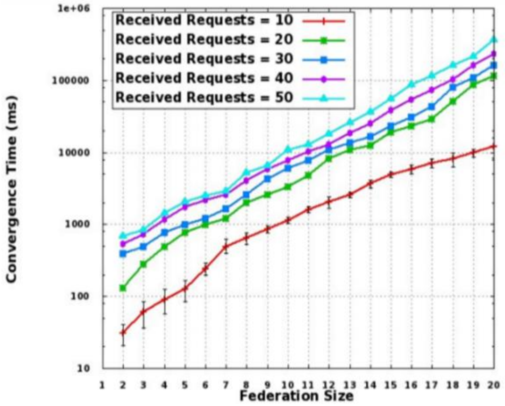

Fig. 7. Comparative Analysis with Katakam Srinivasa Rao vs. the Proposed Work.

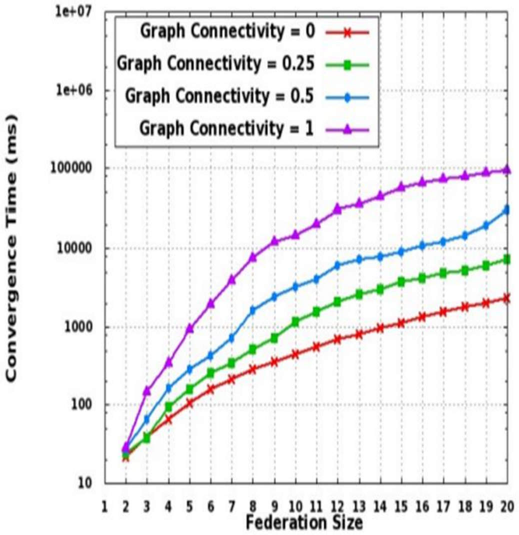

Fig. 8. Comparative Analysis with S.Ye, H. Liu, Y.-W. Leung, and X. Chu VS. our Proposed Work.

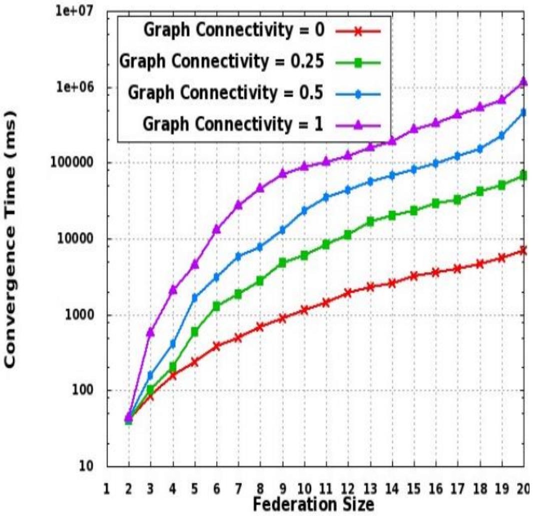

Fig. 9. Comparative Analysis with Vo, Tri Hoang, Woldemar Fuhrmann, Klaus-Peter Fischer-Hellmann, and Steven Furnell vs. the Proposed Work.

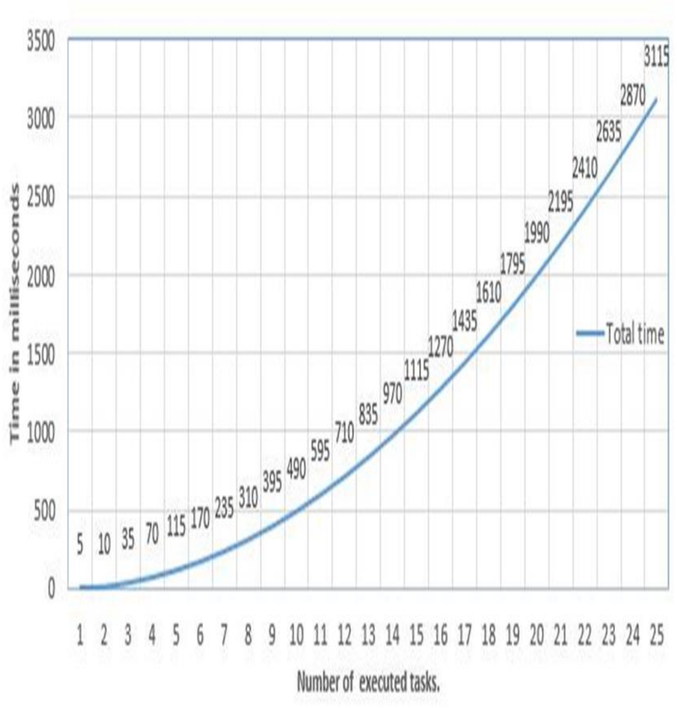

Fig. 10. Execution Time of user Login in the Cloud Federation.

Fig. 10 calculates the execution time to handle the idle UidVM. We have used the number of the on-progress user request (nopur), number of UidVM, and the number of waiting for user request (nwur). The central management system can identify the idle or less loaded UidVM when calculating the on-progress tasks corresponding to the number of UidVM, as described in Algorithm 3.

VI. Conclusion

Global communication has been dealing with one of the major issues – cloud services in terms of security and easy use. To resolve these types of cloud services consumers' complements, the researcher promotes the cloud federation. Cloud federation proposed in this work has resolved the issues mentioned earlier by reducing an execution time and a number of waiting users, and enhancing user request progress. The proposed system has proven that the central management system can identify the idle or less loaded UidVM when calculating 'on progress' tasks corresponding to the number of UidVM, as described in Algorithm 3. This is illustrated by implementing subscribed identities to access cloud resources from multiple cloud service providers. Results clearly indicate the effective reduction of the time consumption when the CSCs use multiple identities to access the resources on multiple CSPs.

Based on all the algorithms and the results obtained are (a) subscribed id is sufficient to access the service without the federated clouds thus reducing the execution time; (b) The work-overload is reduced on the central management system. Fig. 10 shows that 25 LogIn executions are executed in 3115 milliseconds.

Acknowledgment

We thank the Deanship of Scientific Research, Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia for help and support.

TABLE IV. List of Acronyms and Abbreviations

SLA	Service Level Agreement
CSC	Cloud service Consumer
CSP	Cloud Service provider
CSCpc	Cloud Service Consumers pass-code
RSCA	Regional Service Condition Agreement
CFCMS	Cloud Federation Central Management System
UidVM	User identity Verification Module
KDC	Key Distribution Center
CF	Cloud Federation
nopur	number of on progress user request
nwur	number of waiting user request
UidVM	number of user identity Verification module

References

[1] E. U. Directive, "95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data," Official Journal of the EC, vol. 23, 1995.

[2] U. States., "Health insurance portability and accountability act of 1996 [micro form] : conference report (to accompany h.r. 3103)." http://nla.gov.au/nla.catvn4117366, 1996.

[3] S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and Security for Cloud Computing (S. Pearson and G. Yee, eds.), Computer Communications and Networks, pp. 3–42, Springer London, 2013. Computer Science & Information Technology (CS & IT) 147\.

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

[5] Zamani AS, Akhtar MM, Ahmad S. Emerging cloud computing paradigm. International Journal of Computer Science Issues (IJCSI). 2011 Jul 1;8(4):304.

[6] D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz, and A. Scherrer, "Fighting cyber crime and protecting privacy in the cloud." European Parliament, Policy Department C: Citizens' Rights and Constitutional Affairs, October 2012.

[7] M. Y. uddin and S. Ahmad, "A Review on Edge to Cloud: Paradigm Shift from Large Data Centers to Small Centers of Data Everywhere," 2020 International Conference on Inventive Computation Technologies (ICICT), 2020, pp. 318-322, doi: 10.1109/ICICT48043.2020.9112457.

[8] Jha, Sudan, Prashar, Deepak, and Elngar, Ahmed A. 'A Novel Approach Using Modified Filtering Algorithm (MFA) for Effective Completion of Cloud Tasks'. 1 Jan. 2020 : 8409 – 8417.

[9] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," tech. rep., July 2009.

[10] D. Bernstein, "Containers and Cloud: From LXC to Docker to Kubernetes," IEEE Cloud Computing, vol. 1, no. 3, pp. 81-84, 2014.

[11] NIST Special Publication 500–291 version 2, NIST Cloud Computing Standards Roadmap, July 2013, Available at http://www.nist.gov/itl/cloud/publications.cfm.

[12] L. Zhou, V. Varadharajan, and M. Hitchens, "Integrating trust with cryptographic role-based access control for secure cloud data storage," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 560–569, July 2013.

[13] R. Banyal, P. Jain, and V. Jain, "Multi-factor authentication framework for cloud computing," in Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on, pp. 105–110, Sept 2013.

[14] H. Kim and S. Timm, "X.509 authentication and authorization in fermi cloud," in Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, pp. 732–737, Dec 2014.

[15] N. Mimura Gonzalez, M. Torrez Rojas, M. Maciel da Silva, F. Redigolo, T. Melo de Brito Carvalho,C. Miers, M. Naslund, and A. Ahmed, "A framework for authentication and authorization credentials in cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 509–516, July 2013.

[16] B. Tang, R. Sandhu, and Q. Li, "Multi-tenancy authorization models for collaborative cloud services," in Collaboration Technologies and Systems (CTS), 2013 International Conference on, pp. 132–138, May 2013.

[17] M. A. Leandro, T. J. Nascimento, D. R. dos Santos, C. M. Westphall, and C. B. Westphall, "Multitenancy authorization system with federated identity for cloud-based environments using shibboleth," in Proceedings of the 11th International Conference on Networks, ICN 2012, pp. 88–93, 2012.

[18] M. Stihler, A. Santin, A. Marcon, and J. Fraga, "Integral federated identity management for cloud computing," in New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on, pp. 1–5, May 2012.

[19] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in Cloud Computing (M. Jaatun, G. Zhao, and C. Rong, eds.), vol. 5931 of Lecture Notes in Computer Science, pp. 157–166, Springer Berlin Heidelberg, 2009.

[20] S.Ye, H. Liu, Y.-W. Leung, and X. Chu, Reinsurance-Emulated Collaboration Mechanism in Cloud Federation, 2017 IEEE.

[21] Rao, K. S. (2016). A Survey on Authorized Deduplication Techniques in Cloud Computing. International Journal of Engineering Science, 2102.

[22] Vo, Tri Hoang, Woldemar Fuhrmann, Klaus-Peter Fischer-Hellmann, and Steven Furnell. "Identity-as-a-Service: An adaptive security infrastructure and privacy-preserving user identity for the cloud environment." Future Internet 11, no. 5 (2019): 116.

[23] E. Carlini, M. Coppola, P. Dazzi, L. Ricci, and G. Righetti, "Cloud federations in contrail," in Euro-Par 2011: Parallel Processing Workshops (M. Alexander,P. D'Ambra, A. Belloum, G. Bosilca, M. Cannataro, M. Danelutto, B. Di Mar tino, M. Gerndt, E. Jeannot, R. Namyst, J. Roman, S. Scott, J. Traff, G. Vallée, and J. Weidendorfer, eds.), vol. 7155 of Lecture Notes in Computer Science, pp.159–168, Springer Berlin Heidelberg, 2012.

[24] J. Gouveia, P. Crocker, S. Melo De Sousa, and R. Azevedo, "E-id authentication and uniform access to cloud storage service providers," in Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on, vol. 1, pp. 487–492, Dec 2013.

[25] G. Dreo, M. Golling, W. Hommel, and F. Tietze, "Iceman: An architecture for secure federated intercloud identity management," in Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on,pp. 1207–1210, May 2013.

[26] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, HotCloud'09, (Berkeley, CA, USA), USENIX Association, 2009.

[27] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, "Terra: A virtual machine-based platform for trusted computing," in Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles, SOSP '03, (New York, NY, USA), pp. 193–206, ACM, 2003.

[28] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, "Enabling security in cloud storage slas with cloudproof," in Proceedings of the 2011 USENIX Conference on USENIX Annual Technical Conference, USENIX ATC'11, (Berkeley, CA, USA), pp. 31–31, USENIX Association, 2011.

[29] D. Perez-Botero, J. Szefer, and R. B. Lee, "Characterizing hypervisor vulnerabilities in cloud computing servers," in Proceedings of the 2013 International Workshop on Security in Cloud Computing, Cloud Computing '13, (New York, NY, USA), pp. 3–10, ACM, 2013.

[30] J. Sendor, Y. Lehmann, G. Serme, and A. Santana de Oliveira, "Platform level support for authorization in cloud services with oauth 2," in Proceedings of the 2014 IEEE International Conference on Cloud Engineering, IC2E '14, (Washington, DC, USA), pp. 458–465, IEEE Computer Society, 2014.

[31] U. S. F. Law, "Right to financial https://epic.org/privacy/rfpa/, 1978. privacy act of 1978."

[32] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500-292). USA: CreateSpace Independent Publishing Platform, 2012.

[33] "Hypervisors, virtualization, and the cloud: Learn about hypervisors, system virtualization, and how it works in a cloud environment." Retrieved June 2015.

[34] Ahmad S, Afzal MM. A Study and Survey of Security and Privacy issues in Cloud Computing. International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 6 Issue 01, January-2017. http://dx.doi.org/10.17577/IJERTV6IS010311.

[35] Uddin MY, Ahmad S, Afzal MM. Disposable Virtual Machines and Challenges to Digital Forensics Investigation.International Journal of Advanced Computer Science and Applications(IJACSA), 12(2), 2021. http://dx.doi.org/10.14569/IJACSA.2021.0120299.

[36] Ahmad S, Afzal MM. Deployment of Fog and Edge Computing in IoT for Cyber-Physical Infrastructures in the 5G Era. InInternational Conference on Sustainable Communication Networks and Application 2019 Jul 30 (pp. 351-359). Springer, Cham.