International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

# Secure Approach for Cloud: A Comprehensive Survey of Security Measures

**Madhumati B Shinde[1], Premanand P Ghadekar[2]**

**Submitted**: 26/01/2024 **Revised**: 04/03/2024 **Accepted**: 12/03/2024

**Abstract:** Clients using federated learning can learn a global model simultaneously without submitting their own training data to a central server in the cloud. Malicious clients, however, can potentially damage the global model, leading to inaccurate predictions of legal test labels. Federated Learning (FL) protects user privacy by transmitting information from a centralized server to individual endpoints, allowing AI to be applied to areas with sensitive information and heterogeneity. In addition, iterative local model training methods on end-devices allow computing resources to be shared among the involved parties as opposed to depending on a centralized server. One of the extremely fast fields of machine learning, FL is promising to keep up with new regulations protecting user data according to its decentralized data model. In addition to protecting users' confidentiality, FL provides the benefits of ML to specialized areas where there is not enough data for a stand-alone ML model to be developed. As a result of FL's reputation for protecting user privacy, the technology is increasingly being used by industries that process sensitive information. However, Hackers and interested attackers can utilize the federated environment in novel ways because of the increased number of training variants, communications, and the exchange of model parameters. This can be used to influence the ML model's output or gain access to private user data. This research survey explores different technologies emerged for secure cloud environment with FL and ML terminology

***Keywords:*** *Cloud, Federated Learning (FL), Service Level Agreement (SLA), Quality Of Service (QoS)*

## 1. Introduction

The cloud computing concept shows potential since it offers clients with low-cost outsourced services on-demand and on a compensation basis. Infrastructure as a Service (IaaS) providers can be integrated into a federated cloud architecture, creating a heterogeneous and dispersed paradigm for providing infrastructure. Finding the best cloud service for company requirements and determining how to implement it at a reasonable price is an interesting challenge. In a cloud context, problems with data handling, a lack of transparency, and mismanagement concerns can have serious implications for the providers' credibility [2]. It is crucial to establish reliability so that consumers recognize the cloud to be a safe place to store their data. Federal cloud has been the subject of research for the last several years because of its potential to manage huge amounts of information and processing. Confidence management is necessary for cloud services that function in a decentralized manner due to the complexity of service delivery models. A trust relationship must be established between users, Cloud Service Providers (CSPs), and Cloud providers operating in an open, dynamic, and unpredictable cloud computing environment for the effective deployment of federated cloud computing.

To resolve the difficult of data maintenance and data privacy in artificial intelligence, Federated Learning is announced by the google as a Distributed Machine Learning 2016 paradigm. FL allows building the following collaboration models: Federation members ensure preservation of confidential data It is under the control of each participant. FL offers the solution for data silos and destruction issues arising from legislation data sharing should be limited as well as maintained by data owners.

To protect the personal information of the client like any organization or device in FL technology model training would build a global model with a local modernizes. A reliable FL does not share local data externally. An important principles of answerable AI is fronting challenges like responsibility and equity through participation. Different distribution of customer data with different parties some articles present the concept of FL trustworthiness while striving to attain consistently with high training accuracy in Stable AI as a goal it takes into account aspects such as interpretability, fairness, privacy, trustworthiness, accountability and environmental well-being.

FL facilitates artificial intelligence (AI) advantages in domains with sensitive data and heterogeneity and provides a means through which user privacy can be protected via the distribution of data from a central server to end devices . This paradigm emerged for two primary reasons: (1) the inability to store all data on a single server (unlike traditional ML) due to direct access restrictions on such data, and (2) the desire to protect sensitive data by keeping it on the client

*1Dept. of Computer Engineering ,Vishwakarma Institute of Technology(Savitribai Phule Pune University),Pune,India. madhumati.shinde@gmail.com*
*2Dept. of Information Technology, Vishwakarma Institute of Technology(Savitribai Phule Pune University), Pune, India. premanand.ghadekar@vit.edu*

side (edge devices) rather than transmitting it over an asynchronous network connection to the server. Protecting sensitive information makes it possible to apply the many uses of AI made possible by ML models. In addition, iterative local model training procedures on end devices encourage collaboration among stakeholders rather than requiring access to a centralized server for all training needs. One of the fastest-growing areas of ML in recent years is based on the decentralized data notion of FL, which promises to respect new regulations governing user privacy. In addition to protecting users anonymity FL brings the advantages of ML to niche areas where there is not enough data for a stand-alone ML model to be constructed. The federated learning solution with cloud for security and privacy concerns helps implementers/adopters construct a secure environment and researchers choose relevant study domains by highlighting risk variables. The FL examines privacy and security concerns considering federated artificial intelligence's broad deployment.

Safe FL systems must be spirited to outward clients that fail to submit updating the model for aggregation due to problems such as bad network connection, temporary unavailability or power limitations [9]. Peripheral devices with their widespread presence and easy access to the Internet, they are ideal candidates for quality training in various applications. However, participation is limited

potential data leakage and related security issues such as malicious participation, unfair contribution, biased aggregation and central server bottlenecks.

A trusted FL cloud should adhere to the following intentions and goals:

1) Strong security without failure: It protect the system smooth if one component not work

2) Local and Global Guarantees: They offer a robust assurance that superior models result from correct aggregation of numerous native training models without influence.

3) Streamlined model confirmation and auditability: It make easy for users to settle the correctness of model update an easy access to verifiable data for specific update versions.

4) Absolute model update history: Display a internationally uniform record of worldwide model apprises without variations. Within this protocol, each update corresponds a separate record that cannot be edited or deleted once created.

5) Trustworthy client and model identification: Choice trusted clients and models to recover the FL procedure.

## Literature Survey

In this paper [1] authors proposed the CSMIC architecture that is Cloud Service Measurement Index Consortium as an index that to be joined as a formula for Service Measurement Index (SMI) this is valuable to the comparative assessment of the services in cloud. Some challenges are to be considered for understanding the models assessing QoS and for the ranking of cloud providers. As mentioned earlier, the two main concerns in building the proposed framework are the measuring several Service Measurement Index(SMI), Key Performance Indexes (KPIs) and for ranking the services of cloud. Generally, Quality of Service(QoS) models approval for the infrastructure as a service(IaaS) providers based on KPIs of the SMI. An AHP that’s called as Analysis Hierarchical Process centred rank contrivance that is used to estimate services in cloud for different applications according to their Quality of Service requirements. The mechanism proposed also tackle the diverse dimensional tasks of various Quality of Service attributes by provided that a consistent way for the evaluation of comparative grading of the services in cloud for each type of Quality of Service characteristic. However, the ranking algorithm is not equipped with fuzzy sets or fuzzy set inheritance.

The purpose of this document [2] is to explain the nature of threats to cloud infrastructure. Side channel attacks(SCA) are executed locally and take advantage of isolation issues in virtualized environments to obtain sensitive information. Discusses the concept of DSCA that is called as Distributed Side-Channel Attacks and how such spasms interrupt the segregation of virtualized atmospheres like infrastructure in cloud computing. Various countermeasures that can be applied to mitigate attacks in cloud infrastructure are being considered. Numerous virtualization issues are investigated that is related to separation violations inside cloud infrastructure. DSCA (Distributed side channel attacks) have become a vital experiment inside cloud computing organizations with various domain cloud computing architectures and the identified challenge is the design of autonomous mitigation frameworks for numerous Side Channel Attack curriculums in distributed infrastructures in cloud and focus on implementation.

In this paper [3] authors discussed about the IoT ( Internet of Things ) and social grids are driving tremendous development in data transportation flow and the devices which are mobile in nature(mobility), resulting in a race for data communications and secure computing. Customary confidentiality protection approaches are primarily on the basis of data alteration and encryption of data, but these approaches are challenging because they are less protective and complicated to implement. The concept of Differential Privacy is used to enhance data protection. With the most background knowledge, privacy can withstand a wide variety of emerging attacks. Google suggested Federated Learning (FL) in 2016 for secure machine learning. FL is a popular Secure Multiparty Computing (SMC) machine learning framework that permits numerous clients to drill a models together on a central server. Research also includes improving the model for different data processing needs. In addition, the corresponding specialty datasets are used for simulation experiments that provide support technically for other connected areas such as health records, health data segmentation, intelligent electronic and commercial risk forecasting fields

In this article [4] authors discussed about customary central machine learning (ML) methods which cannot provision pervasive dispositions and applications due to the infrastructure insufficiencies like intermittent network connectivity, limited communication bandwidth and tight latency constraints. Another serious issue that is user data privacy and data confidentiality, because data that is used typically comprises sensitive information. Facial images, health information and location-based services may be used for directed social publicity and recommendations, and may pose immediate or potential privacy risks are called sensitive data. An encryption can provide privacy preservation, but it is not fit to poisoning attacks or attacks. Trade-offs between privacy and utility can lead to undesirably bad models.

This article [5] explores how you will trust cloud environments for service utilization. Bionic mechanism is used to build self-organizing systems mechanisms. Suggested trust evaluation method is dynamic based on basic cloud attributes. This method takes into account the factors of the confidence rating. It includes IP, time and behavioural feedback. The data structure used for it includes a trust record table and an access record table. These tables store relationships between ancestor nodes and descendant node with node details. The process of biological evolution is simulated based on trusted information from ancestors of the present node. An ancestor nodes connected graph looks like this: Built to assess overall reliability nodes and Optimal Converted to TSP Problem. The ant colony algorithm determines the order of ancestor nodes. The ancestor node weight influenced by the node trust. The recent node's trust score is expressed as: confidence score and Geometric order. For the each and every factor calculation an existing node trust value is considered. A factor is nothing but weights of predecessor nodes, the existing node's inclusive trust rate is calculated on the basis factors(weights). The biological mechanisms used here are effective. The current node credibility evaluation process looks like in that it considered a complete application of ancestry. Similarly, it shows the trust information and best trust sequence. An ant colony algorithm useful for optimization, when searching node, and it is simple to slip up towards native optima. This can produce unexpected trust score values during the initial reliability assessment, but it can be amended by altering the amount of iterations or search criteria. As the reliance that is nothing but trust information of ancestor nodes increases, assurance score results may be more accurate. Effectively solve common fraud problems.

This article [6] suggested a trust model which is hierarchical level trust model. To find out various cloud service providers authors used the Artificial Bee Colony i.e. ABC algorithm to find different CSPs of the same service, among which the calculated trust score was high and the recommendations from other customers in their feedback were the best. Planned mechanism demonstrated greater accuracy for building trustworthiness, attainment rates, and preventing malicious attacks. Cloud computing operates in a dynamic environment over time Enormous variety of units available this development. At a high level two entities are considered here one is User this entity is the consumer that utilize the services which are provided by the cloud computing environment and second is Services Provider is the person answerable for given the service according to user necessities. It is recommended to maintain trust between different entities hierarchical framework, multi-level trust contract cloud model was proposed. The trust level agreement between different parties that is resolved using two main approach one is Building trust in cloud service providers and second is Maintain user trust. These approaches allow users to Selecting specific services according to their trust score. The proposed study can also help to detect malicious activity and help users make the best decisions for all the services you need. Using the ABC algorithm, quickly search available data and select the best one of them. A user's trust score is calculated based on this. A user ID and the trust score of the cloud service from previous user feedback review is considered for the overall trust score calculations. The experimental trust based model analysis shows that it develops the reliability and accuracy of trust management amongst versatile units in cloud environment.

Authors[7] suggested a dynamic trust rating model for cloud service which is built on privacy consciousness and service level agreement. Here firstly increase the value of the final trust score the proposed model implements comprehensive trust in practical based on a rating consisting of indirect, direct, and reputational trust. Secondly, services from the cloud are classified into five tiers based on their characteristics service options. By analysing SLAs and determining quality, the service allows users to choose the appropriate SLA. Data protection method is proposed on the basis cloud model. Also to dynamically update the trust mechanism is obtainable to describe the trust directly. On the basis public dataset results are obtained that shows the offered model magnificently categorizes the user community based on the preferences of services, that develops the service supplicant's contentment, also prohibit wicked intervention, and this is feasible and accurate.

In this article[8], authors proposed a trust evaluation model. This makes it easier for CSPs to assess and build trust. This ensures that user can participate in a reliable and secure way in cloud federation. This model having two key factors for evaluating trust these are cloud service providers Service Level Agreement and feedback. An attribute that defines security levels is QoP that is nothing but Quality of Protection attributes and the privacy protection mechanisms delivered by CSP are dig out from parsing of the Service Level Agreement document. Here are the combined assurance scores is assessed based on the feedback and mined Quality of Protection parameters. Proof of trust becomes available after evaluation of trust rating that is delivered by model of trust rating. The credentials are swapped amongst CSPs domestically and internationally on a SAML basis. Assertions, or two-way trust, are established between both CSPs. The proposed model was implemented by using, Java and SAML, OpenStack technologies. Further work aims to assess the model for underlying protocol for the diverse threading models.

[9] In this paper authors explore, to successfully save you facts leakage, we advocate a singular framework primarily based totally at the idea of differential privateness (DP), wherein synthetic noises are added to parameters on the customers` facet earlier than aggregating, namely, noising earlier than version accumulation federated Learning (NbAFL). Firstly, author show that the NbAFL can fulfil DP beneathneath wonderful safety ranges by nicely adapting one-of-a-kind variances of synthetic noises. Then expanded a theoretical convergence to sure about the loss functions characteristic of the skilled FL version within side the NbAFL. Precisely, the academic surely exhibits the subsequent 3 key properties: First there is a trade-off among a conjunction overall performance and privateness safety ranges, that is higher convergence overall presentation ends in a decrease safety level, second is given a set privateness safety level, growing the range N of universal customers collaborating in federated learning can be enhance the convergence overall performance and third is an most suitable range accumulation times (conversation circles) in phrases of conjunction overall performance for a specified safety level. Next step to activist a K-purchaser arbitrary scheduling strategy, wherein K customers are arbitrarily decided on from the N universal customers to take part in every aggregation. NbAFL performance further can be extended in different sizes and distributions of customer side data.

In this article [10] authors worked on Cross-silo federated learning this as used to work jointly for training a machine learning model by accumulating local gradient updates from each client without involvement of privacy-sensitive data. FL structures permit clients to cover local gradient updates using additively homomorphic encryption (HE). Homomorphic encryption operations control the training time, while swelling the data transfer amount by two orders of magnitude. author present BatchCrypt, that is system solution for cross-silo FL mainly decreases the encryption and communication upstairs produced by HE. without encrypting separate gradients with full precision, a batch of quantized gradients is encoded into a long integer and encrypt it in unique manner. Gradient-wise mass to be executed on cipher texts of the encoded batches, new quantization and encoding schemes is established along with a new gradient clipping technique. BatchCrypt is applied as a plugin module in FATE(Federated AI Technology Enabler), an industrial cross-silo FL framework.

In [11] this article authors suggest an innovative concept of fine-grained federated Learning for distribute the collective machined learning prototypes on the edge computing servers. A Formal extended definition of smoothly Federate Learning process is presented on the edge computing mobile systems. The basic requirements of smoothly working FL is defined by considering systems personalization, reorganization, stimulus mechanisms, reliance, action monitoring, heterogeneous performance monitoring and the context-consciousness, model of synchronization and communication also efficiency of bandwidth. A block chain-based reputation-aware based concept for smooth FL is presented in direction to confirm reliable combined drill for edge computing in mobile devices systems. The proposed system qualitative comparison is done with correlated work to originate the primary results.

A study proposed in [12] offers a federated cloud utilization in that a cloud adviser manager is in control for tiering and resource provisioning. A Distinguished Service module is assessed on her cloud broker manager and classifies entering users like a Service Level Agreement members or non-SLA fellows. Lively unfastened significance planning has been offered to manage the numerous of services. A secondary Cloud Broker Manager is planned to alleviate CBM overload. In the suggested broker architecture described for the cloud give supports for SLA technique to associate the users and cloud services for informing the provider about the adviser and to develop SLA user performance. To improve scalability and performance new cloud broker architecture including time, task execution , task differentiation and throughput time is recommended. The projected design will help to shrink the starvations of SLA members for the services. To attain determined enactment and SLA members feel less hungry than before existing available cloud broker architecture.

Authors [13] presented adaptive gradient descent scheme for federated learning and variance privacy tools that are appropriate for multiparty collective modelling circumstances. Innovative use of adaptive learning rate algorithms to regulate the gradient descent method that evade ideal(model) overfitting and deviation phenomena to enable federated learning schemes to train efficiently with limited communication costs to improve modelling effectiveness and enactment in multi-party computation scenarios. To adjust to very large-scale dispersed that is distributed safe and secure computing scenarios, this work presents a variance data protection mechanism that resists numerous background spasms.

In this article [14] authors present a new vendor detection algorithm and fuzzy set. A ranking model is projected with a adapted federated style and the performance is Rated. The suggested detection method selects providers on the basis of their service quality. Service Indicators (QoS) recommended to the service's by the Service Measurement Index (SMI). SLA that is service level agreement that provides performance improvements. Add on to this the cost is includes those that represent compliance at the end-user level. Fuzzy set approach is the base for ranking of the services with three general phases: Breaking down the problem, Evaluating priorities and aggregating those priorities. Fuzzy succeeds with a few simple rules. This set can be united through QoS indicators. Weighted Coordinated Queue Scheduling (WTOS) algorithm has been offered to solve the hunger problem in existing architectures Manage requests effectively. The suggested architecture has the following features: Enhanced selection success rate, ordinary response time, and lower overhead architectures that sustained cloud environments.

This paper[15] describes the Federated Cloud Trust Management Framework in cloud for the federation. This framework is recommended to resolve reliability issues and allowing cloud suppliers to magnificently contribute in cloud federations. The projected framework usage the service level agreement for evaluation of trust parameter. Feedback from the customer and her participating CSPs will also be considered. The offered structure is additionally feasible and accurate for trust calculation . A framework has been planned to guarantee Safety of acute and delicate data for customers and CSPs contributing in trusted federation environment. The mechanism used for calculating trust comprises three different parameters SLA parameters, customer feedback, and CSP feedback. The recommended structure can be beneficial to rise the business value of Cloud Service Provider. The Federated Cloud Platform. It not only reduces costs but also serves as a means to rise profits at the same time. Build better business relationships and stay up to date with technology advancements. The work can further be extended by considering detailed architecture of cloud service provider, protocols for trust calculations.

In this article [16] authors propose a system that works on patient centric data in medical field. Lot of predictions can be involving this patient centric big data. Due to this data is firstly divided in to two forms personal information which is sensitive & personal information which is non sensitive. The proposed trust-based access control system that offers authorized and secure access to deliver patient related healthcare data at scale. Patient oriented medical information systems tackle a variety of challenges like reliability, security, integrity, data availability, privacy, patient data access control, etc. was suggested the system provides an method for ensuring the privacy and security of large patient-centric medical data. To provide secure access to PCBMD generated calculations provide correct score accordingly. To prevent users from providing anything Fake feedback about competitors increases the credibility of your feedback. That way you can reward your users efficiently provide honest approvals and penalize users for false recommendations. To provide secure access to PCBMD also proposes a Secure Data Protection Scheme (PIPPS) established on user's exact trust scores. Untrusted users can be prevented by PIPPS so, accessing sensitive patient information is escaped. The proposed system scheme make subtle information available only to the anticipated beneficiary without disclosing their personal data. The planned system is safe, efficient as well as reliable, as related to other present systems.

In this article[17] authors tackle the issue of safe and clear usage of cloud services. Federated Identity Management is introduced for a lively trust model in cloud. Fuzzy cognitive mapslogic is used for modelling and evaluating trust relations between entities which are involved in cloud federation under the model known as federated identity management systems. Secure & dynamic trustworthiness technique enables the trust relationships amongst anonymous things, also increases the flexibility and scalability of federated identity management systems, and allows positioning and maintenance in cloud environments.

This paper authors [18] provided dynamic trust rating scheme which is multi-dimensional in nature that adjusts reliability of CSPs and customers here the perspective of numerous cloud units is taken in to the consideration. To select the preferred quality of service desires and legitimate customers anticipated by the CSP achieves the reliability. As per the given results of this paper expose that the planned scheme is robust and dynamic in distinguishing between untrusted and trusted customers and cloud service providers.

This article[19] introduces the collaboration Big. Little subdivision model architecture that allows effectual federated learning for the applications of AIoT. This architecture is inspired by BranchyNet, this is an approach leverages deep neural, that uses prediction of multiple branches. A considered network model for cloud and AIoT devices is DNN. Two branches are there in the Big. Little branch model that is big branch & little branch. The branch which is deployed on the cloud is big branch for strengthened cloud prediction accuracy, and to fit for AIoT devices the little branches are used . With AIoT Device cannot make predictions with great certainty smaller local branches will turn to larger branches for more purposes implication. To improve both early exit and predictive accuracy rate the Big.Little industry model is used in that, authors proposed two stages of training. A meeting scheme that considers regional characteristics and a description of the AIoT scenario. The results obtained Efficienc from real AIoT environments. Validity of Approaches for Predictive Accuracy average inference time. Suggested two-step training, and the schemes for Coinference significantly improves the predictions Accuracy of a single AIoT device with small branches, This reduces the average inference time below that. Support from large branch offices deployed in the cloud.

This article [20] expose PPFL structure in federated learning to preserve the privacy for the mobile devices also to prevent privacy leakages while working in the FL environment. The TEE(Trusted Execution Environments) technique is utilized on mobile edge devices, mainly its purpose is at client side for the native training & at server side for secure accumulation because of this model incline apprises are concealed from rivals. The challenge of limited stream storage size TEE trains each model using greedy stratified training and layer up until convergence within the confidence region. Especially $PPFL$ model can protect well skilled model and reconstruction of data, assets inference, Belonging Inference Attack. By considering CPU time, memory size as a limited asset and their usage with energy utilization a PPFL suggested model can preserve membership attack as well as train the model for data reconstruction.

In this article [21] a block-chain centred federated learning using SMPC (Secure multiparty computing protocol) model validation is proposed for poison attack on the medical system. Firstly, Machine learning models are plaid from Federated Learning participants via scrambled interpretation process and then eliminate the cooperated model. After the spatial models of the participants have been verified, the model is directed to the block chain node to be firmly accumulated. To test the suggested framework different medical datasets are used. The proposed structure can further be expanded for an effective compromise mechanism to decrease computational and energy assets as well as for to build efficient communication mechanism between involved participants in FL.

In this [22] authors suggest a new method that uses deep learning and technique of block chain for health care records privacy protection. Federated Learning that is included with block chain & cryptography to classify the health records uses neural network model. Distributed network for healthcare record by the use of block chain can proves the data protection. The propose work expanded with deep reinforcement learning with block chain integrity.

In this [24] authors suggested a secure architecture for the IoT with use of Ethereum Blockchain which is concern with most of the security parameters in the recommended architecture. The suggested model is light weighted secure architecture for IoT technology. The problem called as single point authentication in existing IoT networks can be solved by decentralized Blockchain technique . A Smart Home System as a demonstrative case study has been applied for wider IoT applications. The two parameters measured are temperature and intrusion detection. The Qualitative assessment of the offered architecture highlights how it tackles various attacks & deals with challenges in IoT network. An attacks are evaluated in the given model like Man in the middle attack and DoS attack also Centralized authentication process followed to confirm the access control of the devices in network. The model can be release with latest Ethereum that can provide more efficiency, trust ,reliability, less time and less electricity consumption.

## Experimental results discussion

An overview of trust built mechanism inside federated cloud environment on the basis of literature survey is shown here by considering the parameters like data security, dynamicity, data integrity, availability and reliability. As the results given in the table 1 shows that major factors highlighted while work in federated cloud environment. To develop a trustworthiness amongst cloud service provider & cloud service user that is evaluated by considering different aspects that adhere to trust. A deficiency of appropriate cloud security can rigorously affect cloud service suppliers and their consumers. So, the secure cloud is the practice for securing computer networks as well as data of the user in cloud computing surroundings. Following parameters can further be prolonged with secure network constraints like firewalls, proxies and gateways to protect the data from hackers. Now days Cloud computing and machine learning are evolving technologies they play a vital part in company's overall progression. So these technologies together become more powerful machine learning helps to make an intelligent machines and software while cloud computing offers storage and security for the data to smooth handling of the environment.

**Table1**.Experimental results discussion based on different parameters

| Main Factor | Author names | Security | Reliability | Integrity | Availability | Dynamicity |
|---|---|---|---|---|---|---|
| **Trust Evaluation** | Saurabh Kumar et al.(2013) | ✗ | ✓ | ✗ | ✓ | ✗ |
| | C. S. Rajarajeswari el al.(2014) | ✗ | ✓ | ✗ | ✗ | ✗ |
| | Kanwal A et al(2014) | ✗ | ✗ | ✓ | ✓ | ✗ |
| | L. Aruna et al.(2016) | ✓ | ✗ | ✗ | ✓ | ✗ |
| | Mohammad-Mahdi et al.(2018) | ✓ | ✗ | ✗ | ✓ | ✗ |
| | Wang Y et al.(2018) | ✓ | ✓ | ✗ | ✓ | ✗ |
| | Ma S, Shuai et al.(2018) | ✓ | ✓ | ✗ | ✓ | ✗ |
| | Bendiab K et al(2018) | ✓ | ✓ | ✗ | ✗ | ✗ |
| | Kaushik S et al.(2019) | ✓ | ✗ | ✓ | ✗ | ✗ |
| | K. Wei et al.(2020) | ✓ | ✓ | ✗ | ✓ | ✗ |
| | C. Zhang et al.(2020) | ✓ | ✗ | ✗ | ✓ | ✓ |
| | Xinqian Zhang et al.(2020) | ✓ | ✗ | ✗ | ✓ | ✓ |
| | Xiang Wu a et al.(2021) | ✓ | ✓ | ✗ | ✓ | ✓ |
| | Lingjuan Lyu et al.(2022) | ✓ | ✗ | ✗ | ✗ | ✓ |
| | Xiang Wu et al.(2022) | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Fan Mo et al.(2021) | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Aditya Pribadi et al.(2022) | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Jafar A et al.(2023) | ✓ | ✓ | ✓ | ✓ | ✓ |

## Conclusion

This survey research identifies establishment of a trusted environment is an important factor to evaluate trustworthiness between cloud service providers to enable involvement in federation for the consumption of computing resources in cloud environment. Various factors are considered like SLA, QoS in federated learning cloud environment to develop trust on cloud service provider as well as privacy preserving mechanisms are taken in to consideration for data security. Cloud computing is becoming more and more popular now days. However, the security risk continues to impede cloud computing's progress. Data privacy & trust development in cloud system by using distributed computing that is federated learning is highlighted. To achieve the privacy general cryptography methods and algorithms are used to improve the privacy, accuracy, scalability the research can be further extended to apply deep neural network and reinforcement learning with block chain methodology in federated learning as a major concern.

## References

[1] Saurabh Kumar Garg a, Steve Versteeg b, Rajkumar Buyya a, “A framework for ranking of cloud computing services,” Elsevier, 2013

[2] Mohammad-Mahdi Bazm & Marc Lacoste & Mario Südholt & Jean-Marc Menaud “Isolation in cloud

computing infrastructures: new security challenges”2018.

[3] Xiang Wu a, Yongting Zhang a , Minyu Shi a , Pei Li b , Ruirui Li c , Neal N. Xiong“An adaptive federated learning scheme with differential privacy preserving,” Elsevier, 2021.

[4] Lingjuan Lyu , Han Yu , Xingjun Ma, Chen Chen, Lichao Sun, Jun Zhao, Qiang Yang , Fellow, IEEE, and Philip S. Yu, Fellow, IEEE, “Privacy and Robustness in Federated Learning: Attacks and Defenses,” unpublished.2022

[5] Ma S, Shuai X, Zhou Z, Qiao K (2018) Bionic mechanism based dynamic trust evaluation method in cloud environment. In: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)

[6] Kaushik S, Gandhi C (2019) “Multi-level trust agreement in cloud environment. “,2019 Twelfth International Conference on Contemporary Computing (IC3), pp 1–5

[7] Wang Y, Wen J, Zhou W, Luo F (2018) A novel dynamic cloud service trust evaluation model in cloud computing. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)

[8] Kanwal A, Masood R, Shibli MA (2014) Evaluation and establishment of trust in cloud federation. In: Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. Association for Computing Machinery

[9] K. Wei et al., Federated learning with differential privacy: Algorithms and performance analysis, IEEE Trans. Inf. Forensics Secure. (2020)

[10] C. Zhang et al., Batch crypt: Efficient homomorphic encryption for cross-silo federated learning, in: {USENIX}, 2020

[11] Muhammad Habib ur Rehman, Khaled Salah, Ernesto Damiani, Davor Svetinovic ”Towards Blockchain-Based Reputation-Aware Federated Learning” August 24,2020 ,IEEE Explore

[12] C. S. Rajarajeswari , M. Aramudhan “Ranking Model for SLA Resource Provisioning Management”2014.

[13] Xiang Wu a, Yongting Zhang a, Minyu Shi a, Pei Li b, Ruirui Li c, Neal N. Xion “An adaptive federated learning scheme with differential privacy preserving”,2022

[14] [14] L. Aruna1, M. Aramudhan2 ,“framework for ranking service providers of federated cloud architecture using fuzzy sets”,2016

[15] Rabia Latif · Syeda Hadia Afzaal · Seemab Latif “A novel cloud management framework for trust establishment and evaluation in a federated cloud environment”,2021.

[16] Navroop Kaur, Yachana, Sandeep K. Sood ,“A Trustworthy System for Secure Access to Patient Centric Sensitive Information”.

[17] Bendiab K, Shiaeles S, Boucherkha S (2018) A new dynamic trust model for “on cloud” federated identity management. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS).

[18] Challagidad PS, Birje MN (2019) Determination of trustworthiness of cloud service provider and cloud customer. In: 2019 5th International Conference on Advanced Computing Communication Systems (ICACCS).

[19] Xinqian Zhang, Ming Hu Student Member, IEEE, Jun Xia, Tongquan Wei Senior Member, IEEE, Mingsong Chen Senior Member, IEEE, and Shiyan Hu Senior Member, IEEE(2020) “Efficient Federated Learning for Cloud-Based AIoT Applications”.

[20] Fan Mo, Hamed Haddadi, Kleomenis Katevas, Eduard Marin, Diego Perino, Nicolas Kourtellis, “PPFL: Privacy-preserving Federated Learning with Trusted Execution Environments”,2021.

[21] Aditya Pribadi Kalapaaking, Ibrahim Khalil, Xun Y, “Blockchain-based Federated Learning with SMPC Model Verification Against Poisoning Attack for Healthcare Systems”, ieee transactions on emerging topics in computing 2022.

[22] Jafar A. Alzubi , Senior Member, IEEE, Omar A. Alzubi , Member, IEEE, Ashish Singh , and Manikandan Ramachandran, “Cloud-IIoT-Based Electronic Health Record Privacy-Preserving by CNN and Blockchain-Enabled Federated Learning”January 2023.

[23] Runhua Xu, Nathalie Baracaldo, Yi Zhou, Ali Anwar, Swanand Kadhe, and Heiko Ludwig, “DeTrust-FL: Privacy-Preserving Federated Learning in Decentralized Trust Setting”,2022.

[24] PremanandGhadekar, NiketDoke, SushmitaKaneri, Varsha Jha,”Secure Access Control to IoT Devices using Blockchain”, International Journal of Recent Technology and Engineering (IJRTE),2019