International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: 27 January 2024 ***Revised:*** 12 February 2024 ***Accepted:*** 14 March 2024

Secure Data Transactions in Mobile Cloud Computing using FAAS

G. Matheen Fathima[1]
Research Scholar
School of Computer Science Engineering & Information Science,
Presidency University, Itgalpura, Rajanukunte, Yelahanka, Bangalore - 560064, India.
matheen.20233CSE0025@presidencyuniversity.in

L.Shakkeera[2]
Professor
School of Computer Science Engineering & Information Science,
Presidency University, Itgalpura, Rajanukunte, Yelahanka, Bangalore - 560064, India.
shakkeera.l@presidencyuniversity.in

Sharmasth Vali.Y[3]
Assistant Professor (Sel. Grade),
School of Computer Science Engineering & Information Science,
Presidency University, Itgalpura, Rajanukunte, Yelahanka, Bangalore - 560064, India.
sharmasth.vali@presidencyuniversity.in

Abstract— In recent times, security breaches have come to light in mobile cloud transactions, raising concerns about the vulnerability of data stored in mobile clouds. This data is at risk of tampering or unauthorized modification by external users, especially because it resides within a public cloud infrastructure managed by organizations. Such breaches can significantly impact the authenticity and integrity of the stored data. Mobile cloud computing (MCC) is a technology designed to facilitate the transfer of data and communication with end-users over the internet through a mobile cloud infrastructure. To address the urgent need to secure and protect data stored in mobile clouds, we propose the implementation of the Mobile Cloud-Security Model (MCSM). This innovative model is poised to provide an elevated level of data security and integrity for user data by harnessing the power of Federated Learning (FL) and Federation as a Service (FaaS). Federated Learning (FL) seamlessly integrates into the data training process, culminating in the generation of a model using the data hosted in the mobile cloud. This pioneering approach enables collaborative model training while steadfastly upholding data privacy and security. Federation as a Service (FaaS) represents a cloud-based solution that streamlines collaboration and data sharing among diverse organizations or entities. It simplifies the complex processes of configuring trust relationships, managing identities, and establishing data exchange agreements among federated entities, all made possible through the provision of Service Level Agreements (SLAs) for data stored in the mobile cloud. The user data stored in the mobile cloud will be retrieved using Machine Learning (ML) algorithms that learn from user data. Subsequently, this data is offloaded from the edge devices. The outcome of this research is to maintain user data within the FAAS cloud service with higher-level of confidentiality, security and integrity of user's data.

Keywords-Mobile cloud Security model (MCSM); Data Integrity; Data Privacy; Federated Learning; Federation as a Service; Machine Learning;

1. INTRODUCTION

Mobile Cloud Computing (MCC) [1] is important because it enhances accessibility and scalability for users. It allows for data and applications to be stored and processed in remote servers, reducing the burden on mobile devices and enabling users to access their resources from anywhere. This improves convenience and efficiency, making it a valuable technology for modern computing. MCC is a robust innovation that harnesses the flexible assets in diverse cloud and network innovation. It aims to provide Infinite capabilities, storage capacity, and portability offered to a diverse array of mobile devices, accessible through either Ethernet or the internet, regardless of varying surroundings and platforms. This model operates based on a usage-based payment model and is categorized into three distinct service models: Mobile as a Service Consumer (MaaSC), Mobile as a Service Provider (MaaSP), and Mobile as a Service Broker (MaaSB).

Data security in mobile cloud environments [2][3] for users brings forth a multitude of critical challenges and concerns. These issues emerge from the intricate balance between the demand for seamless data access and sharing and the crucial need to safeguard sensitive information. The primary concerns are the data privacy and access control. The challenge here is to find an intermediary between the

convenience of mobile cloud access and the necessity to control who can access specific data. To address this, organizations must implement robust access control mechanisms aimed at preventing unauthorized users from tampering with or extracting sensitive information. Data Encryption plays a pivotal role in this scenario, ensuring that data remains secure both in transit and at rest, effectively thwarting potential interception or theft. Identity and Authentication are critical components of data security. Verifying the identity of users accessing data on mobile cloud platforms is imperative. Implementing multi-factor authentication (MFA) and enforcing strong password policies can significantly enhance the security of the authentication process. In the data training process, the Mobile Cloud (MC) often needs to fetch data from the cloudlet using Machine Learning (ML) algorithms. This is because the cloud may not have sufficient storage capacity to handle the data, necessitating the use of ML algorithms to predict and retrieve data efficiently from the edge devices.

To tackle these challenges effectively, the implementation of Federated Learning (FL) and Federation as a Service (FAAS) for user data stored in the MC becomes crucial. The FAAS service provides a Service Level Agreement (SLA) contract [4], which serves as a protective shield for the data, essentially forming a member contract with a pay-for-use demand structure in the cloud. This approach not only addresses the critical issues surrounding data security in mobile cloud environments but also optimizes data access, utilization, and protection through the integration of advanced technologies like FL and FAAS services.

2. RELATED WORK

Guanjin Qu, Naichuan Cui, Huaming Wu, Ruidong Li, and Yuemin Ding have proposed an approached named “ChainFL: A Simulation Platform for Joint Federated Learning and Blockchain in Edge/Cloud Computing Environments” [5]. ChainFL (CFL) serves as a versatile simulator tool capable of constructing an edge computing environment that integrates seamlessly with IoT devices, it is remaining adaptable with both FL and BC technologies. Its primary objective is to assists the implementation of security-oriented offloading algorithms The advantage of CFL is its ability to be utilized by an FL, offering heightened security features that effectively tackle the challenges presented by vast amounts of data and potential cyberattacks within the Industrial Internet of Things (IIoT) domain. However, it's important to note a disadvantage: implementing CFL in serverless edge computing is essential for achieving greater scalability, reliability, and cost reduction, especially in scenarios involving tasks with stringent latency requirements.

Huan Zhou, Zhenning Wang, Hantong Zheng, Shibo He, and Mianxiong Dong have proposed an approach in their paper titled "Cost Minimization-Oriented Computation Offloading and Service Caching in Mobile Cloud-Edge Computing: An A3C-Based Approach" [6]. This paper primarily focuses on introducing a mechanism called DRLCOSCM. The goal of this mechanism Optimizing offloading, decisions, strategies for caching services and allocating resources need optimization. The objective is to reduce expenses associated with CSC while still meeting in delay requirements of mobile users. One notable advantage of the DRLCOSCM approach is that it formulates the optimization issues as an occurrence of Mixed Integer Non-Linear Programming (MINLP). Additionally, this paper proposes an Algorithm based on A3C to effectively address and rectify this optimization issue. However, a notable disadvantage of this approach is the challenge of determining a specific methodology for implementing a deep learning algorithm among the various available options.

Zhou Su, Yuntao Wang, Tom H. Luan, Ning Zhang, Feng Li, Tao Chen, Hui Cao have presented a paper titled "Secure and Efficient Federated Learning for Smart Grid with Edge-Cloud Collaboration" [7]. This paper introduces a scheme aimed at ensuring both the security and efficiency of FL of the context of Smart Grids (SG) that collaborate with edge and cloud resources. The primary focus of this paper is to establish the sharing of confidential energy data. within SG’s that utilize edge and cloud resources. This framework leverages edge-cloud assistance to facilitate federated learning, enabling efficient and privacy-protecting sharing of confidential energy data among the participants in SG. One significant advantage of this approach is its ability to use EDOs (Evolutionary Differential Operators) for exchanging high-quality local model updates, ultimately improving optimizing the coherence of communication. Additionally, the paper introduces an algorithm for incentives based on DRL designed to protect participants private information. However, the paper acknowledges certain limitations, such as the need to further investigate on the development of a model for evaluating local performance within the framework of differential privacy (DP) using gradient perturbation, in the context of AIoT.

Huijin Cao, Jun Cai have presented a paper titled "Distributed Multiuser Computation Offloading for Cloudlet-Based Mobile Cloud Computing: A Game-Theoretic Machine Learning Approach" [8]. This paper addresses the issues of decision-making for multi-user delegating computation in a non-cooperative game setting and aims to find the NEP in a fully distributed environment. To achieve this FDCO algorithm that exploits the MLtechnology. One notable advantage of this FDCO algorithm is its ability to optimize the use of advantageous cloudlets for processing tasks on mobile devices. It optimizes both the number of mobile devices benefiting from cloudlet computing and the system-wide execution cost. However, it's important to acknowledge a potential limitation of this approach. In the future, if mobile

device users exhibit heterogeneous characteristics, this system may not effectively support the Nash equilibrium point, as it was originally designed for a homogeneous group of mobile users.

Ji Liu, Lei Mo, Sijia Yang, Jingbo Zhou, Shilei Ji, Haoyi Xiong, Dejing Dou (June 2023) "Data Placement for Multi-Tenant Data Federation on the Cloud" [9]. The approach they propose aims to enable cloud-based data processing using information originating from various entities. This technique comprises a data federation platform known as FedCube (FC), coupled with a data placement algorithm based on Lyapunov principles. FC facilitates cloud-based data simplification. Data placement algorithm is employed to devise a strategy for partitioning and storing data in the cloud, aiming to accomplish various goals while staying within the limitations specified in a multi-objective cost framework. Advantage of their work is the experimental evidence demonstrating a significant reduction in total costs (up to 69.8%) compared to existing methods. However, a disadvantage is the challenge of selecting a specific methodology for implementing a Lyapunov algorithm over others.

Wei Yang Bryan Lim, Nguyen Cong Luong, Dinh Thai Hoang, Yutao Jiao, Ying-Chang Liang, Qiang Yang, Dusit Niyato , Chunyan Miao (2020) "Federated Learning in Mobile Edge Networks: A Comprehensive Survey" [10]. This paper explores the concept of Mobile edge computing (MEC) as a way to extend intelligence to the network edge, where data originates. The traditional ML technologies in MEN often need the sharing of individualized information with external parties, posing privacy concerns. Federated Learning (FL) presents a solution in which end devices utilize their local data for training an ML model as requested by the server. Rather than transmitting raw data, these devices transmitting model updates to the server for consolidation. FL offers an advantage on being an authorize technology for MEN, allowing collaborative ML model training and facilitating DL for network optimization. Nevertheless, Scaling the implementation of FL faces challenges related to factors to consider include communication expenses, resource distribution, and privacy and security issues.

Weimin Li, Qin Li, Lin Chen, Fan Wu, Ju Ren (September 2022) have presented a paper titled "A Storage Resource Collaboration Model Among Edge Nodes in Edge Federation Service" [11]. In the model for efficient storage resource collaboration, the emphasis lies in optimizing the choice of cooperative edge nodes and the distribution of storage resources among these nodes. This approach aims to provide effective and achieving equilibrium in storage service solutions is a key goal. Specifically, resolving the selection of collaborative edge nodes for storage involves addressing a multi-objective integer linear programming problem. Additionally, a pricing mechanism based on a greedy storage resource allocation auction is employed. Notably, experimental results demonstrate that these methods efficiently address the challenge of storage resource collaboration among edge nodes in an edge federation service. However, there is room for improvement in future work. One potential avenue for enhancement involves exploring the application of DRL approaches for tackling the challenge of allocating storage resources collaboratively within the context of edge federation services, with the potential to improve the overall performance of the storage resource collaboration model.

Xiaofeng Lu, Yuying Liao, Pietro Lio, And Pan Hui (February 25, 2020) "Privacy-Preserving Asynchronous Federated Learning Mechanism for Edge Network Computing" [12]. The proposed approach is the PPAFLM designed to enable numerous edge nodes to engage in efficient FL while safeguarding their personal information. One advantage of PAFLM is that it provides learners with increased freedom and privacy protection without sacrificing the improving the precision of their training. Participants can gain insights from their own confidential datasets on a local level. However, there is room for further improvement in future work. Specifically, we plan to explore various attenuation functions and seek a more suitable attenuation function to meet the requirements of the system.

Jiang Zhang, Zhenfeng Zhang, Hui Guo (November 2017) "Towards Secure Data Distribution Systems in Mobile Cloud Computing" [13]. In this paper, we utilize a range of cryptographic techniques, including an innovative type-based proxy re-encryption method, to create a secure and efficient data distribution system within Mobile Cloud Computing. This system offers privacy of data, data validation, data verification, and adaptable data distribution with access management. The advantage of this approach is the creation of an operational data distribution system for MCC that operates without the involvement of any trusted third party. It also offers several valuable features, such as enhancing data confidentiality, data integrity, data verification, real-time data updates and removals, and precise access control. However, the challenge that remains is the selection of a specific methodology for implementing a TB-PRE scheme algorithm over other available options.

Yufeng Zhan, Jie Zhang, Zicong Hong, Leijie Wu, Peng Li, and Song Guo have presented a paper titled "A Survey of Incentive Mechanism Design for Federated Learning" [14]. The central focus of this paper is on the importance of effectively motivating encouraging clients to engage actively and consistently in FL through the use of incentive mechanisms. One notable advantage of incorporating incentive mechanisms is that it encourages participants to actively engage in federated learning by offering them a share

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: 27 January 2024 Revised: 12 February 2024 Accepted: 14 March 2024

of the revenue generated when their local datasets are used. Consequently, it becomes crucial to assess the contributions of various data providers to ensure the revenue generated through the educational system are dispersed fairly and relevantly. However, a notable challenge highlighted in the paper is the need to implement incentive mechanism designs that cater to Federated learning involving multiple parties, federated learning incentivized by rewards, and the incorporation of security measures to guarantee the effectiveness of these incentive mechanism.

3. TECHNOLOGIES AND SERVICES IN MCC

3.1 Resource Allocation

Resource allocation [15] and scheduling strategy maximize the cloud provider's profit and satisfy SLA using dynamic rank-based resource allocation and scheduling algorithm. The cloud users enable the users to set up and boot the resources based on their requirements and then, users can pay merely for the utilized resources from the cloud. Adaptive resource allocation utilizes task execution times and preemptive scheduling to address resource contention issues and enhance resource utilization. Cloud users can configure and launch resources according to their needs, enabling them to pay only for the resources they actually use from the cloud.

3.2 Computational Offloading

Computation offloading [16] involves transferring computationally intensive application components to a remote server. In MCC, the task scheduling [17] requires the decision to offload is determined by the device's attributes. The scheduling technique involves dividing the application into mobile tasks and cloud tasks prior to scheduling it on the cloud server. The scheduling process for a given task depends on the preceding task within the application. However, the current task scheduling and allocation algorithm only takes into account the execution completion time. This approach results in an overall increase in the application completion time for mobile application requests, thereby diminishing the performance of the entire system.

3.3 Optimization Techniques

Optimization [18] focuses on the several factors such as resource provisioning, task scheduling, cost, and cloud service optimization. It aims at resolving over-provisioning and under-provisioning problems, improving the service quality, and reducing cost and response time. The optimization involves in both the processes, including scheduling the tasks and allocating the cloud resources. The Energy Consumption Optimization for Cloud Computing based on the Task Tolerance (ECCT) approach aims to enhance resource utilization and minimize power consumption through a resource scheduling optimization algorithm. This optimization relies on the increasing task tolerance for resource execution in cloud computing.

3.4 Workflow Management

The workflow management [19] is divided into 3 categories, the objective of minimizing the execution cost and overall completion time, and optimally selecting the non-dominated solutions. The workflow tasks into the number of levels and then schedules the workflow tasks based on the levels in private and public cloud. At each level, independent tasks are to be executed in parallel. Two resource allocation strategies are available, depending on budget constraints. These strategies decompose the scheduling problem of non-deterministic workflows into a series of deterministic sub-workflows. Complex workflows consist of recursively parallel sub-flows of tasks, which pose challenges in deploying them on heterogeneous cloud computing nodes.

3.5 Services in MCC

Mobile cloud computing [20] provides essential services, including data storage, app hosting, content delivery, device management, sync, location-based features, augmented reality, AI integration, IoT support, and robust security.These services improve mobile user experiences by offering flexibility, scalability, and access to potent cloud resources. Businesses can achieve cost savings by adopting Mobile Cloud Computing. Entrepreneurs benefit from the portability of cloud technology, enhancing work efficiency. Mobile cloud consumers enjoy access to a broader array of features on their smartphones. Developers can tap into larger markets by leveraging the mobile cloud.

4. SECURE MOBILE CLOUD DATA

Security is a crucial concept in Mobile Cloud Computing (MCC). If a user's data is tampered, hacked, or altered by a third party, it undermines the convenience of storing data securely through MCC. Nowadays, most businesses store their organizational data in the cloud. To ensure efficient security of data and confidentiality of data within the MCC environment, the proposed new methodology aims to enhance data security and privacy within the MCC framework.

The Mobile Cloud Security Model (MCSM) represents a proposed methodology for facilitating secure data transactions within the mobile cloud environment. The process begins with mobile users logging into the MC environment using their credentials. The database stores these user credentials and verifies whether they are authorized user, and then granting access to their stored data within the MC. Edge devices play a pivotal role in fetching and fortifying data within the mobile cloud, enhancing its security. The Machine learning algorithm which trains and learns from the data currently stored in the cloud and fetching the data based on user’s requirement. Following the data offloading stage, the data proceeds to the Federated Learning (FL) phase. During this FL phase, all nodes learn from the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 1
Article Received: 27 January 2024 Revised: 12 February 2024 Accepted: 14 March 2024

data and then the data is stored locally on mobile devices, ultimately generating a model. This generated model is been placed on the Global Model Server, which iteratively trains user data using the generated model. The user's data remains in an encrypted format, inaccessible to third-party users. The security and confidentiality of user data are efficiently upheld through an SLA contract, guaranteeing a higher level of data security and data privacy while employing a pay-as-you-use model. Leveraging the SLA contract, the encrypted data is further fortified and seamlessly integrated into Federation-as-a-Service (FaaS) [11], ensuring the utmost protection and data integrity.

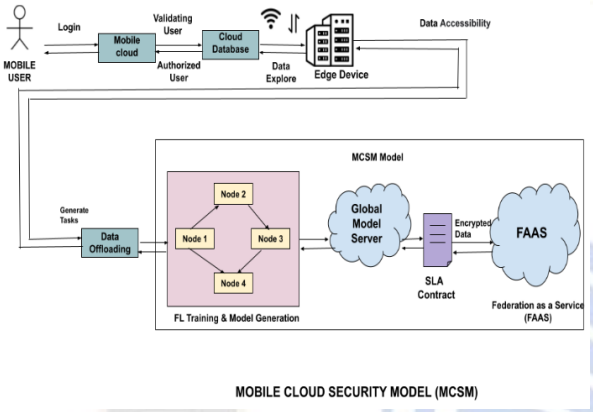

Fig 4.1 Mobile Cloud Security Model (MCSM)

In Fig 4.1 defines the FAAS (Federation as a Service) maintains highly sensitive user data in accordance with the SLA (Service Level Agreement) contract established between users and cloud federations. It offers FAAS for securing and storing data in the mobile cloud. Users can access their data from any location, and they have complete control over the data stored within the FAAS service. This model efficiently manages the user's data in the MC environment and provides an assurance of maintaining the user's data with a higher-level of security of user's data.

A. FEDERATED LEARNING (FL)

Federated learning (FL), also known as collaborative learning, represents a machine learning technique that is gaining prominence in today's data-driven approach. This algorithm operates across numerous decentralized edges, ensuring that raw data remains securely housed within mobile devices, thus preserving the privacy and security of sensitive information. This process begins with the algorithm training on these dispersed mobile devices, each with its unique dataset. After training, the model derived from this process is then centralized and placed on the Global Model Server (GMS). This server acts as a repository for the collective knowledge gleaned from the individual edge devices. Federated learning bears resemblance to blockchain-consensus algorithms in its operation. Within this network-driven paradigm, data operations and training take place in a distributed fashion, allowing for collaborative learning while safeguarding data privacy. This approach holds great promise for industries and applications where data security and privacy are paramount concerns.

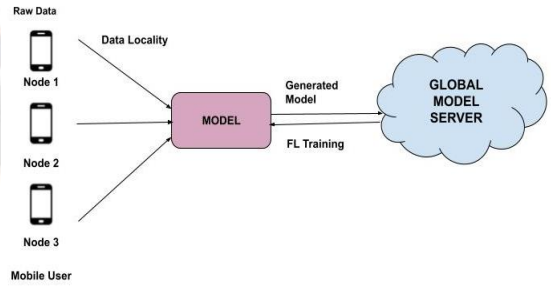

Fig 4.1.2 Federated Learning

In Fig 4.1.2 defines the multiple user nodes (raw data) are been trained using FL and the generated model is been placed in Global model server. Iteratively the generated model trains the raw data of the nodes and generates a new model recursively. Each time a user adds data to the mobile cloud, a model is generated and stored in GMS. The data collected by the edge devices are trained and a model is been obtained, the generated model will be maintained in the GMS, it iteratively trains the models added locally to the mobile devices.

B. FEDERATION AS A SERVICE (FAAS)

The SUNFISH introduces an innovative cloud federation solution known as Federation-as-a-Service (FAAS). This novel approach facilitates the secure establishment and administration of cloud federations, offering a seamless service for clouds. Within these cloud federations, the data being managed is of a highly sensitive nature. FAAS plays a crucial role by providing a robust level of assurance regarding the member contracts governing data handling and security. One notable feature of FAAS is its versatility. It can seamlessly integrate into the mobile cloud environment, allowing for the secure management of user data stored in mobile cloud services while adhering to Service Level Agreement (SLA) contracts. This integration enhances both user data privacy and security in the mobile cloud, making FAAS a valuable solution for organizations seeking to safeguard sensitive information in a connected world.

An SLA functions as a formal agreement between a service provider and the recipient, delineating their shared understanding of the services provided and the associated benefits. FaaS, or Federation-as-a-Service, enables individual clouds to unite for the purpose of sharing and utilizing their computing resources, services, and data. These collective entities represent the offerings of the federation, accessible to each member while adhering to security and SLA policies

defined by individual clouds and enforced by the platform. Each individual cloud offering a service is obligated to furnish the security and SLA policies that govern the provisioning of paid service. The platform ensures the effective enforcement of these policies, with the capability to monitor security and performance metrics and adjust the SLA and access control policies currently in effect accordingly.

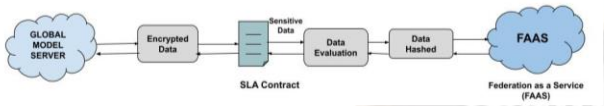

Fig 4.1.3 Federation as a Service

In Fig 4.1.3 defines the model obtained from the global model server is encrypted and stored using the SLA contract inorder to secure and protect the privacy of user data (sensitive data). The FAAS service upholds an SLA to ensure enhanced data assurance and security for user data stored in the FAAS cloud service. This data will be further hashed and maintained in the FAAS has a service to the user. The user will be charged for the data fortify in the FAAS. The FAAS service offers a commitment to safeguarding user data within the MC environment.

5. MOBILE CLOUD APPLICATION

An Elastic Application is a software application designed to scale and adapt to changing workloads. It can automatically allocate and deallocate resources based on demand, ensuring optimal performance and resource utilization. A collaborative approach in mobile cloud involves integrating mobile computing and cloud computing technologies to enhance collaboration and resource sharing. This approach is commonly employed to enhance the functionality and efficiency of mobile applications by leveraging cloud resources. We can optimize the mobile cloud according to user demands by employing elastic applications for resource allocation when handling uploaded data. This approach helps balance the user load when accessing the mobile cloud environment. Additionally, we can implement a collaborative approach to efficiently manage user requests for processing and storing their data in the FAAS.

6. CONCLUSION

The MCSM model is designed to provide an end-to-end data security and seamless data accessibility within the mobile cloud environment. It accomplishes this by employing machine learning algorithms to train the dataset, allowing for the rapid retrieval of information in response to the user queries. By leveraging machine learning algorithms, user queries can be processed with remarkable efficiency, resulting in reduced network traffic and minimized data congestion. The goal of this research is to establish and maintain Secured Data Communication (SDC) within the mobile cloud infrastructure, all achieved through the integration of a Federated Learning and Federation as a service. This innovative approach not only ensures the privacy and security of data but also optimizes data retrieval processes, ultimately enhancing the overall user experience and the efficiency of mobile cloud services.

REFERENCES

[1] Niroshinie Fernando, Seng W. Loke, Wenny Rahayu, “Mobile cloud computing: A survey”, Future Generation Computer Systems, Volume 29, Issue 1,2013, Pages 84-106, (DOI: org/10.1016/j.future.2012.05.023).

[2] Shakkeera. L, Saranya. A, “Efficient Collaborative Key Management Protocol for Secure Mobile Cloud Data Storage”, in International Conference on Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, vol 846. Springer, Singapore, 9 September, 2018 (DOI: 10.1007/978-981-13-2182-5_4).

[3] Shakkeera. L, Saranya. A, Sharmasth Vali. Y, “Secure Collaborative Key Management System for Mobile Cloud Data Storage” in International Journal of Engineering and Advanced Technology (IJEAT), Vol. 8, No. 5S3, pp:214-225, July 2019.(DOI:10.35940/ijeat.E1049.0785S319).

[4] Shakkeera. L, Latha Tamilselvan, “Satisfying Sla Objectives Of Seamless Execution Of Mobile Applications In Cloud With Net Profit” in Journal of Theoretical and Applied Information Technology, Vol.95. No 11, pp: 2577-2588, 15 June 2017.

[5] G. Qu, N. Cui, H. Wu, R. Li and Y. Ding, "ChainFL: A Simulation Platform for Joint Federated Learning and Blockchain in Edge/Cloud Computing Environments," in IEEE Transactions on Industrial Informatics, vol. 18, no. 5, pp. 3572-3581, May 2022, doi: 10.1109/TII.2021.3117481.

[6] H. Zhou, Z. Wang, H. Zheng, S. He and M. Dong, "Cost Minimization-Oriented Computation Offloading and Service Caching in Mobile Cloud-Edge Computing: An A3C-Based Approach," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 3, pp. 1326-1338, 1 May-June 2023, doi: 10.1109/TNSE.2023.3255544.

[7] Z. Su et al., "Secure and Efficient Federated Learning for Smart Grid With Edge-Cloud Collaboration," in IEEE Transactions on Industrial Informatics, vol. 18, no. 2, pp. 1333-1344, Feb. 2022, doi: 10.1109/TII.2021.3095506.

[8] H. Cao and J. Cai, "Distributed Multiuser Computation Offloading for Cloudlet-Based Mobile Cloud Computing: A Game-Theoretic Machine Learning Approach," in IEEE Transactions on Vehicular Technology, vol. 67, no. 1, pp. 752-764, Jan. 2018, doi: 10.1109/TVT.2017.2740724.

[9] J. Liu et al., "Data Placement for Multi-Tenant Data Federation on the Cloud," in IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 1414-1429, 1 April-June 2023, doi: 10.1109/TCC.2021.3136577.

[10] W. Y. B. Lim et al., "Federated Learning in Mobile Edge Networks: A Comprehensive Survey," in IEEE

Communications Surveys & Tutorials, vol. 22, no. 3, pp. 2031-2063, thirdquarter 2020, doi: 10.1109/COMST.2020.2986024.

[11] W. Li, Q. Li, L. Chen, F. Wu and J. Ren, "A Storage Resource Collaboration Model Among Edge Nodes in Edge Federation Service," in IEEE Transactions on Vehicular Technology, vol. 71, no. 9, pp. 9212-9224, Sept. 2022, doi: 10.1109/TVT.2022.3179363.

[12] X. Lu, Y. Liao, P. Lio and P. Hui, "Privacy-Preserving Asynchronous Federated Learning Mechanism for Edge Network Computing," in IEEE Access, vol. 8, pp. 48970-48981, 2020, doi: 10.1109/ACCESS.2020.2978082.

[13] J. Zhang, Z. Zhang and H. Guo, "Towards Secure Data Distribution Systems in Mobile Cloud Computing," in IEEE Transactions on Mobile Computing, vol. 16, no. 11, pp. 3222-3235, 1 Nov. 2017, doi: 10.1109/TMC.2017.2687931.

[14] Y. Zhan, J. Zhang, Z. Hong, L. Wu, P. Li and S. Guo, "A Survey of Incentive Mechanism Design for Federated Learning," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 2, pp. 1035-1044, 1 April-June 2022, doi:10.1109/TETC.2021.3063517.

[15] Shakkeera. L, Latha Tamilselvan, "Towards Maximum Resource Utilization and Optimal Task Execution for Gaming IoT Workflow in Mobile Cloud" in International Journal of Intelligent Engineering & Systems, 2017,Vol.10 Issue 1, p134-143. 10p. (DOI: 10.22266/ijies2017.0228.15)

[16] Karthik Kumar, Jibang Liu, Yung-Hsiang Lu, and Bharat Bhargava, "A survey of computation offloading for mobile systems", Springer transaction on Mobile Networks and Applications, Vol.18, No.1, pp.129-140, 2012.

[17] Shakkeera. L, Latha Tamilselvan , "QoS and load balancing aware task scheduling framework for mobile cloud computing environment" in International Journal of Wireless and Mobile Computing, 2016, Vol.10, No.4, pp: 309316 (DOI: 10.1504/IJWMC.2016.078201)

[18] Wang Hinayana, Xue Lin, and Massoud Pedram, "A Nested two stage game-based optimization framework in mobile cloud computing system", IEEE 7th International Symposium on Service Oriented System Engineering (SOSE), pp.494-502, 2013.

[19] Liu L, Zhang M, Lin Y, and Qin L, "A survey on workflow management and scheduling in cloud computing", 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), pp.837-846, 2014.

[20] Niroshinie Fernando, Seng W. Loke, and Wenny Rahayu, "Mobile cloud computing: A survey", Elsevier transaction on Future Generation Computer Systems, Vol.29, pp.84–106, 2013.